NO PLACE TO HIDE

EDWARD SNOWDEN, THE NSA, AND
THE U. S. SURVEILLANCE STATE

GLENN GREENWALD

This book is dedicated to all those
who have sought to shine a light
on the US government's secret
mass surveillance systems,
particularly the courageous
whistle-blowers who have risked
their liberty to do so.

3

COLLECT IT ALL

The archive of documents Edward Snowden had assembled was stunning in both size and scope. Even as someone who had spent years writing about the dangers of secret US surveillance, I found the sheer vastness of the spying system genuinely shocking, all the more so because it had clearly been implemented with virtually no accountability, no transparency, and no limits.

The thousands of discrete surveillance programs described by the archive were never intended by those who implemented them to become public knowledge. Many of the programs were aimed at the American population, but dozens of countries around the planet—including democracies typically considered US allies, such as France, Brazil, India, and Germany—were also targets of indiscriminate mass surveillance.

Snowden's archive was elegantly organized, but its size and complexity made it extremely difficult to process. The tens of thousands of NSA documents in it had been produced by virtually every unit and subdivision within the sprawling agency, and it also contained some files from closely aligned foreign intelligence agencies. The documents were startlingly recent: mostly from 2011 and 2012, and many from 2013. Some even dated from March and April of that year, just months before we met Snowden in Hong Kong.

The vast majority of the files in the archive were designated "top secret." Most of those were marked "FVEY," meaning that they were approved for distribution only to the NSA's four closest surveillance allies, the "Five Eyes" English-speaking alliance composed of Britain, Canada, Australia, and New Zealand. Others were meant for US eyes only, marked "NOFORN" for "no foreign distribution." Certain documents, such as the FISA court order allowing collection of telephone records and Obama's presidential directive to prepare offensive cyber-operations, were among the US government's most closely held secrets.

Deciphering the archive and the NSA's language involved a steep learning curve. The agency communicates with itself and its partners in an idiosyncratic language of its own, a lingo that is bureaucratic and stilted yet at times boastful and even snarky. Most of the documents were also quite technical, filled with forbidding acronyms and code names, and sometimes required that other documents be read first before they could be understood.

But Snowden had anticipated the problem, providing glossaries of acronyms and program names, as well as internal agency dictionaries for terms of art. Still, some documents were impenetrable on the first, second, or even third reading. Their significance emerged only after I had put together different parts of other papers and consulted with some of the world's foremost experts on surveillance, cryptography, hacking, the history of the NSA, and the legal framework governing American spying.

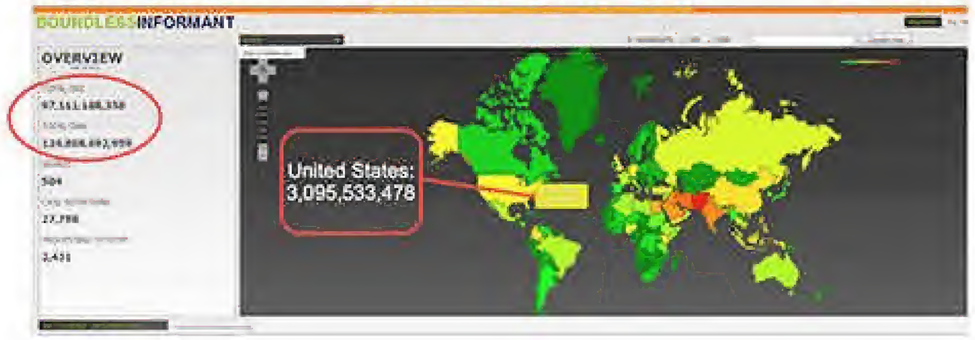
Compounding the difficulty was the fact that the mountains of documents were often organized not by subject but by branch of the agency where they had originated, and dramatic revelations were mixed in with large amounts of banal or highly technical material. Although the *Guardian* devised a program to search through the files by keyword, which was of great help, that program was far from perfect. The process of digesting the archive was painstakingly slow, and many months after we first received the documents, some terms and programs still required further reporting before they could be safely and coherently disclosed.

Despite such problems, though, Snowden's files indisputably laid bare a complex web of surveillance aimed at Americans (who are explicitly beyond the NSA's mission) and non-Americans alike. The archive revealed the technical means used to intercept communications: the NSA's tapping of Internet servers, satellites, underwater fiber-optic cables, local and foreign telephone systems, and personal computers. It identified individuals targeted for extremely invasive forms of spying, a list that ranged from alleged terrorists and criminal suspects to the democratically elected leaders of the nation's allies and even ordinary American citizens. And it shed light on the NSA's overall strategies and goals.

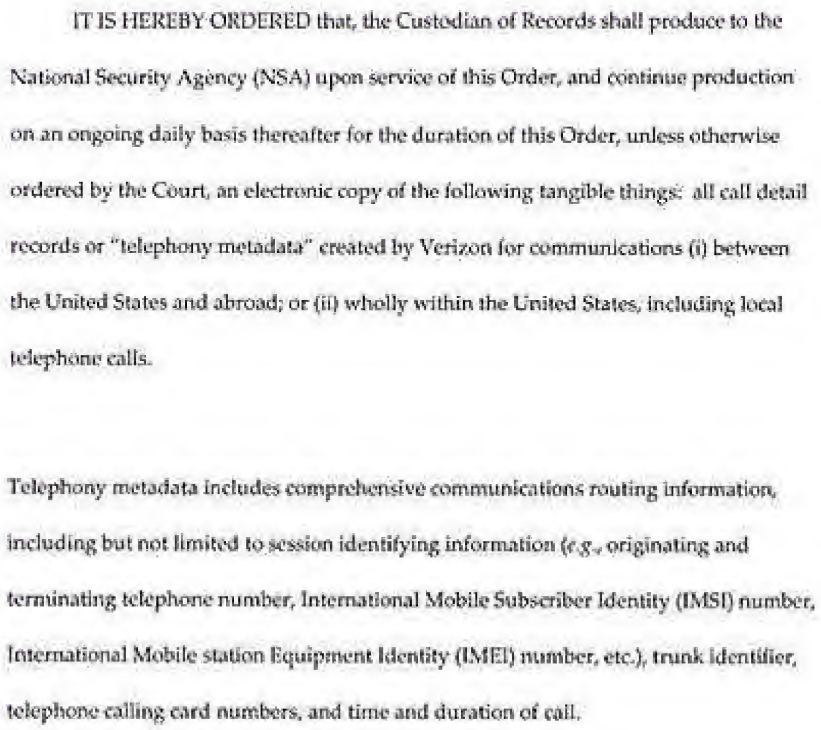
Snowden had placed crucial, overarching documents at the front of the archive, flagging them as especially important. These files disclosed the agency's extraordinary reach, as well as its deceit and even criminality. The BOUNDLESS INFORMANT program was one of the first such revelations, showing that the NSA counts all the telephone calls and emails collected every day from around the world with mathematical exactitude. Snowden had placed these files so prominently not only because they quantified the volume of calls and emails collected and stored by the NSA—literally billions each day—but also because they proved that NSA chief Keith Alexander and other officials had lied to Congress. Repeatedly, NSA officials had claimed that they were incapable of providing specific numbers—exactly the data that BOUNDLESS INFORMANT was constructed to assemble.

For the one-month period beginning March 8, 2013, for example, a BOUNDLESS INFORMANT slide showed that a single unit of the NSA, Global Access Operations, had collected data on more than 3 billion telephone calls and emails that had passed through the US telecommunications system. ("DNR," or "Dialed Number Recognition," refers to telephone calls; "DNI," or "Digital Network Intelligence," refers to Internet-based communications such as emails.) That exceeded the collection from the systems each of Russia, Mexico, and virtually all the countries in Europe, and was roughly equal to the collection of data from China.

Overall, in just thirty days the unit had collected data on more than 97 billion emails and 124 billion phone calls from around the world. Another BOUNDLESS INFORMANT document detailed the international data collected in a single thirty-day period from Germany (500 million), Brazil (2.3 billion), and India (13.5 billion). And yet other files showed collection of metadata in cooperation with the governments of France (70 million), Spain (60 million), Italy (47 million), the Netherlands (1.8 million), Norway (33 million), and Denmark (23 million).



Despite the NSA's statutorily defined focus on "foreign intelligence," the documents confirmed that the American public was an equally important target for the secret surveillance. Nothing made that clearer than the April 25, 2013, top secret order from the FISA court compelling Verizon to turn over to the NSA all information about its American customers' telephone calls, the "telephony metadata." Marked "NOFORN," the language of the order was as clear as it was absolute:



IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.

Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.

This bulk telephone collection program was one of the most significant discoveries in an archive suffused with all types of covert surveillance programs—from the large-scale PRISM (involving collection of data directly from the servers of the world's biggest Internet companies) and PROJECT BULLRUN, a joint effort between the NSA and its British counterpart, the Government Communications Headquarters (GCHQ), to defeat the most common forms of encryption used to safeguard online transactions, to smaller-scale enterprises with names that reflect the contemptuous and boastful spirit of supremacy behind them: EGOTISTICAL GIRAFFE, which targets the Tor browser that is meant to enable anonymity in online browsing; MUSCULAR, a means to invade the private networks of Google and Yahoo!; and OLYMPIA, Canada's program to surveil the Brazilian Ministry of Mines and Energy.

Some of the surveillance was ostensibly devoted to terrorism suspects. But great quantities of the programs manifestly had nothing to do with national security. The documents left no doubt that the NSA was equally involved in economic espionage, diplomatic spying, and suspicionless surveillance aimed at entire populations.

Taken in its entirety, the Snowden archive led to an ultimately simple conclusion: the US government had built a system that has as its goal the complete elimination of electronic privacy worldwide. Far from hyperbole, that is the literal, explicitly stated aim of the surveillance state: to collect, store, monitor, and analyze all electronic communication by all people around the globe. The agency is devoted to one overarching mission: to prevent the slightest piece of electronic communication from evading its systemic grasp.

This self-imposed mandate requires endlessly expanding the NSA's reach. Every day, the NSA works to identify electronic communications that are not being collected and stored and then develops new technologies and methods to rectify the deficiency. The agency regards itself as needing no specific justification to collect any particular electronic communication, nor any grounds for regarding its targets with suspicion. What the NSA calls "SIGINT"—all signals intelligence—is its target. And the mere fact that it has the capability to collect those communications has become one rationale for doing so.

* * *

A military branch of the Pentagon, the NSA is the largest intelligence agency in the world, with the majority of its surveillance work conducted through the Five Eyes alliance. Until the spring of 2014, when controversy over the Snowden stories became increasingly intense, the agency was headed by four-star general Keith B. Alexander, who had overseen it for the previous nine years, aggressively increasing the NSA's size and influence during his tenure. In the process, Alexander became what reporter James Bamford described as "the most powerful intelligence chief in the nation's history."

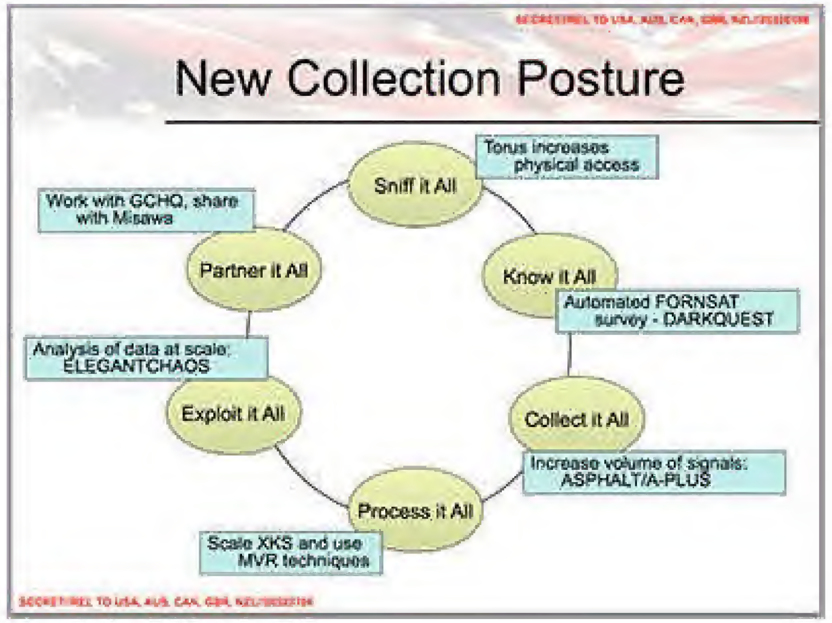
The NSA "was already a data behemoth when Alexander took over," *Foreign Policy* reporter Shane Harris noted, "but under his watch, the breadth, scale, and ambition of its mission have expanded beyond anything ever contemplated by his predecessors." Never before had "one agency of the U.S. government had the capacity, as well as the legal authority, to collect and store so much electronic information." A former administration official who worked with the NSA chief told Harris that "Alexander's strategy" was clear: "I need to get all of the data." And, Harris added, "He wants to hang on to it for as long as he can."

Alexander's personal motto, "Collect it all," perfectly conveys the central purpose of the NSA. He first put this philosophy into practice in 2005 while collecting signals intelligence relating to the occupation of Iraq. As the *Washington Post* reported in 2013, Alexander grew dissatisfied with the limited focus of American military intelligence, which targeted only suspected insurgents and other threats to US forces, an approach that the newly appointed NSA chief viewed as too constraining. "He wanted everything: Every Iraqi text message, phone call, and e-mail that could be vacuumed up by the agency's powerful computers." So the government deployed technological methods indiscriminately to collect all communications data from the entire Iraqi population.

Alexander then conceived of applying this system of ubiquitous surveillance—originally created for a foreign population in an active war zone—to American citizens. "And, as he did in Iraq, Alexander has pushed hard for everything he can get," the *Post* reported: "tools, resources, and the legal authority to collect and store vast quantities of raw information on American and foreign communications." Thus, "in his eight years at the helm of the country's electronic surveillance agency, Alexander, 61, has quietly presided over a revolution in the government's ability to scoop up information in the name of national security."

Alexander's reputation as a surveillance extremist is well documented. In describing his "all-out, barely legal drive to build the ultimate spy machine," *Foreign Policy* called him "the cowboy of the NSA." Even Bush-era CIA and NSA chief General Michael Hayden—who himself oversaw the implementation of Bush's illegal warrantless eavesdropping program and is notorious for his aggressive militarism—often had "heartburn" over Alexander's no-holds-barred approach, according to *Foreign Policy*. A former intelligence official characterized Alexander's view: "Let's not worry about the law. Let's just figure out how to get the job done." The *Post* similarly noted that "even his defenders say Alexander's aggressiveness has sometimes taken him to the outer edge of his legal authority."

Although some of the more extreme statements from Alexander—such as his blunt question "Why can't we collect all the signals, all the time?," which he reportedly asked during a 2008 visit to Britain's GCHQ—have been dismissed by agency spokespeople as mere lighthearted quips taken out of context, the agency's own documents demonstrate that Alexander was not joking. A top secret presentation to the 2011 annual conference of the Five Eyes alliance, for instance, shows that the NSA has explicitly embraced Alexander's motto of omniscience as its core purpose:



SECRET//REL TO USA, AUS, CAN, GBR, NZL//[illegible]

New Collection Posture

Sniff it All

Torus increases physical access

Know it All

Automated FORNSAT survey - DARKQUEST

Collect it All

Increase volume of signals: ASPHALT/A-PLUS

Process it All

Scale XKS and use MVR techniques

Exploit it All

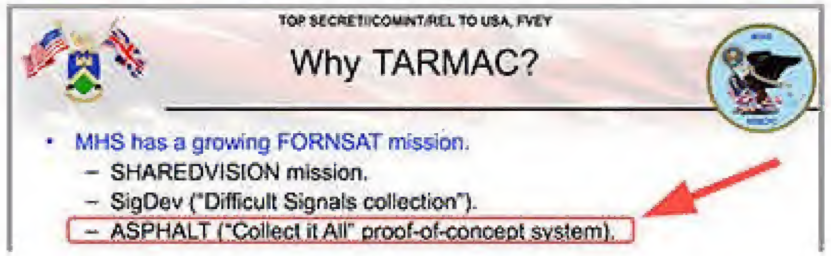
Analysis of data at scale: ELEGANTCHAOS

Partner it All

Work with GCHQ, share with Misawa

SECRET//REL TO USA, AUS, CAN, GBR, NZL//[illegible]

A 2010 document presented to the Five Eyes conference by the GCHQ—referring to its ongoing program to intercept satellite communications, code-named TARMAC—makes it clear that the British spy agency also uses this phrase to describe its mission:



TOP SECRET//COMINT//REL TO USA, FVEY

Why TARMAC?

- MHS has a growing FORNSAT mission.
  - SHAREDVISION mission.
  - SigDev ("Difficult Signals collection").
  - ASPHALT ("Collect it All" proof-of-concept system).

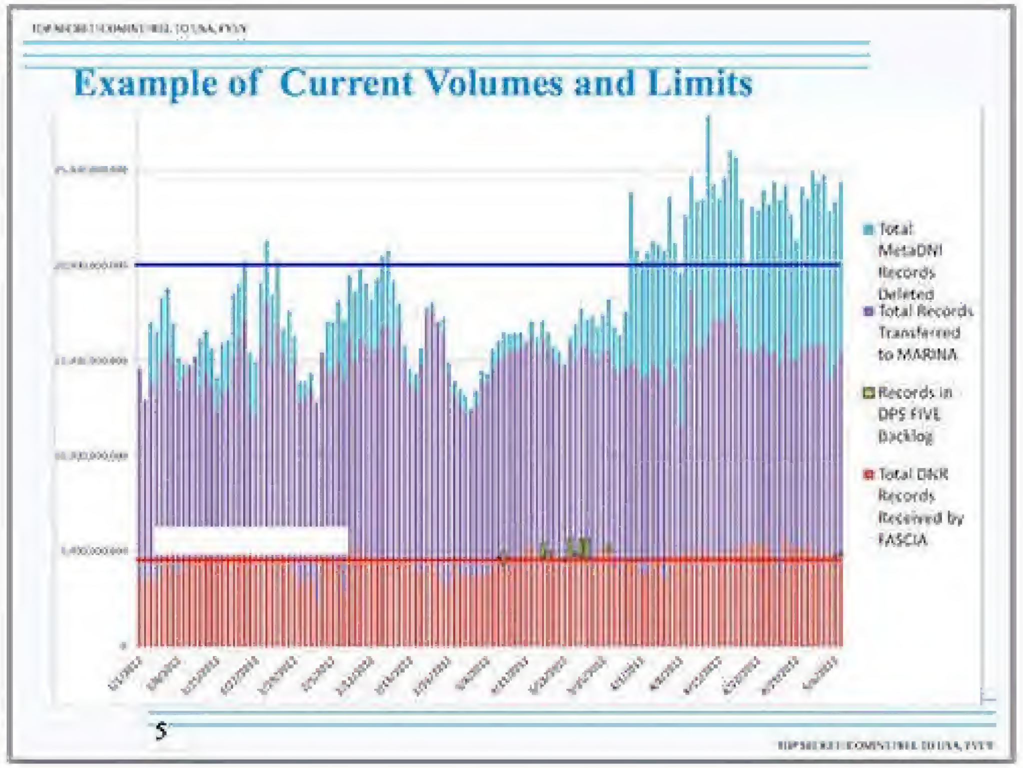
Even routine internal NSA memoranda invoke the slogan to justify expanding the agency's capabilities. One 2009 memo from the technical director of the NSA's Mission Operations, for example, touts recent improvements to the agency's collection site in Misawa, Japan:

Future Plans (U)

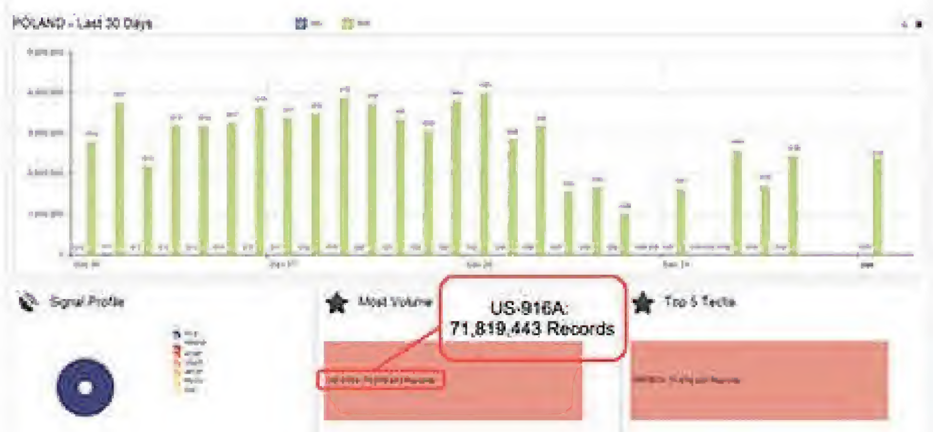
(TS//SI//REL) In the future, MSOC hopes to expand the number of WORDGOPHER platforms to enable demodulation of thousands of additional low-rate carriers.

These targets are ideally suited for software demodulation. Additionally, MSOC has developed a capability to automatically scan and demodulate signals as they activate on the satellites. There are a multitude of possibilities, bringing our enterprise one step closer to "collecting it all."

Far from being a frivolous quip, "collect it all" defines the NSA's aspiration, and it is a goal the NSA is increasingly closer to reaching. The quantity of telephone calls, emails, online chats, online activities, and telephonic metadata collected by the agency is staggering. Indeed, the NSA frequently, as one 2012 document put it, "collects far more content than is routinely useful to analysts." As of mid-2012, the agency was processing more than twenty billion communications events (both Internet and telephone) from around the world *each day*:



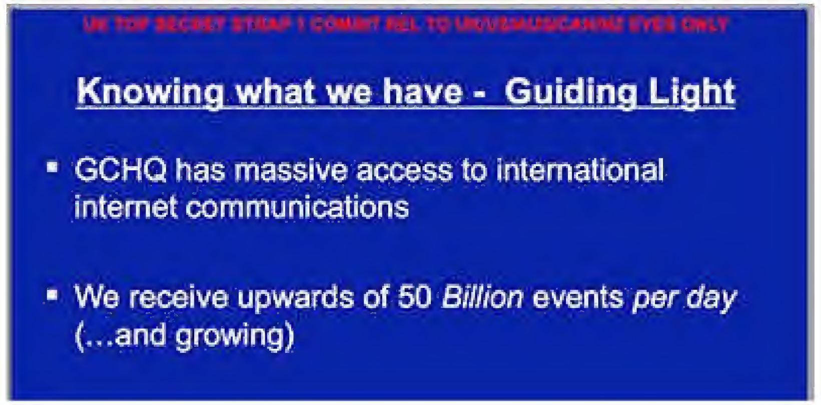
For each individual country, the NSA also produces a daily breakdown quantifying the number of calls and emails collected. The chart below, for Poland, shows more than three million telephone calls on some days, for a thirty-day total of seventy-one million:



The domestic total collected by the NSA is equally stunning. Even prior to Snowden's revelations, the *Washington Post* reported in 2010 that "every day, collection systems at the National Security Agency intercept and store 1.7 billion emails, phone calls, and other types of communications" from Americans. William Binney, a mathematician who worked for the NSA for three decades and resigned in the wake of 9/11 in protest over the agency's increasing domestic focus, has likewise made numerous statements about the quantities of US data collected. In a 2012 interview with *Democracy Now!*, Binney said that "they've assembled on the order of 20 trillion transactions about U.S. citizens with other U.S. citizens."

After Snowden's revelations, the *Wall Street Journal* reported that the overall interception system of the NSA "has the capacity to reach roughly 75% of all U.S. Internet traffic in the hunt for foreign intelligence, including a wide array of communications by foreigners and Americans." Speaking anonymously, current and former NSA officials told the *Journal* that in some cases the NSA "retains the written content of emails sent between citizens within the U.S. and also filters domestic phone calls made with Internet technology."

Britain's GCHQ similarly collects such a great quantity of communications data that it can barely store what it has. As one 2011 document prepared by the British put it:

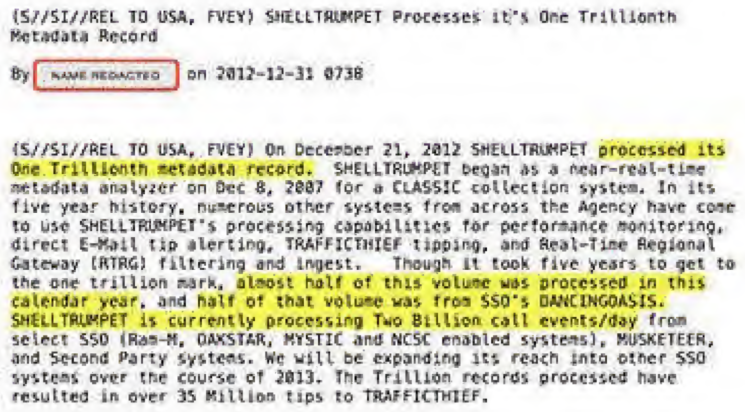


UK TOP SECRET STRAP 1 COMINT REL TO UK/US/AUS/CAN/NZ EYES ONLY

Knowing what we have - Guiding Light

- GCHQ has massive access to international internet communications
- We receive upwards of 50 *Billion* events *per day* (...and growing)

So fixated is the NSA on collecting it all that the Snowden archive is sprinkled with celebratory internal memos heralding particular collection milestones. This December 2012 entry from an internal messaging board, for instance, proudly proclaims that the SHELLTRUMPET program has processed its one trillionth record:



(S//SI//REL TO USA, FVEY) SHELLTRUMPET Processes it's One Trillionth Metadata Record

By NAME REDACTED on 2012-12-31 0738

(S//SI//REL TO USA, FVEY) On December 21, 2012 SHELLTRUMPET processed its One Trillionth metadata record. SHELLTRUMPET began as a near-real-time metadata analyzer on Dec 8, 2007 for a CLASSIC collection system. In its five year history, numerous other systems from across the Agency have come to use SHELLTRUMPET's processing capabilities for performance monitoring, direct E-Mail tip alerting, TRAFFICTHIEF tipping, and Real-Time Regional Gateway (RTRG) filtering and ingest. Though it took five years to get to the one trillion mark, almost half of this volume was processed in this calendar year, and half of that volume was from SSO's DANCINGOASIS. SHELLTRUMPET is currently processing Two Billion call events/day from select SSO (Ram-M, OAKSTAR, MYSTIC and NCSC enabled systems), MUSKETEER, and Second Party systems. We will be expanding its reach into other SSO systems over the course of 2013. The Trillion records processed have resulted in over 35 Million tips to TRAFFICTHIEF.

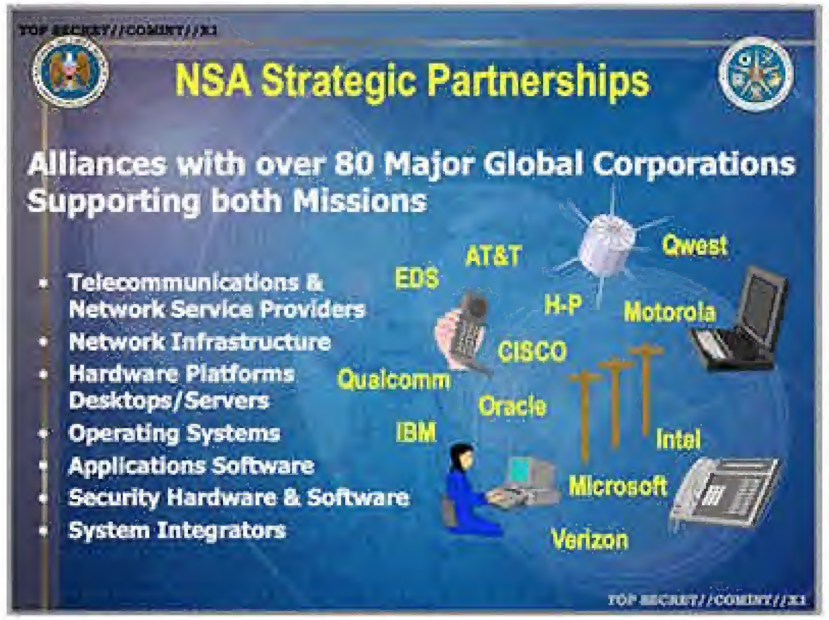
* * *

To collect such vast quantities of communications, the NSA relies on a multitude of methods. These include tapping directly into fiber-optic lines (including underwater cables) used to transmit international communications; redirecting messages into NSA repositories when they traverse the US system, as most worldwide communications do; and cooperating with the intelligence services in other countries. With increasing frequency, the agency also relies on Internet companies and telecoms, which indispensably pass on information they have collected about their own customers.

While the NSA is officially a public agency, it has countless overlapping partnerships with private sector corporations, and many of its core functions have been outsourced. The NSA itself employs roughly thirty thousand people, but the agency also has contracts for some sixty thousand employees of private corporations, who often provide essential services. Snowden himself was actually employed not by the NSA but by the Dell Corporation and the large defense contractor Booz Allen Hamilton. Still, he, like many other private contractors, worked in the NSA offices, on its core functions, with access to its secrets.

According to Tim Shorrock, who has long chronicled the NSA-corporate relationship, "70 percent of our national intelligence budget is being spent on the private sector." When Michael Hayden said that "the largest concentration of cyber power on the planet is the intersection of the Baltimore Parkway and Maryland Route 32," Shorrock noted, "he was referring not to the NSA itself but to the business park about a mile down the road from the giant black edifice that houses NSA's headquarters in Fort Meade, Md. There, all of NSA's major contractors, from Booz to SAIC to Northrop Grumman, carry out their surveillance and intelligence work for the agency."

These corporate partnerships extend beyond intelligence and defense contractors to include the world's largest and most important Internet corporations and telecoms, precisely those companies that handle the bulk of the world's communications and can facilitate access to private exchanges. After describing the agency's missions of "Defense (Protect U.S. Telecommunications and Computer Systems Against Exploitation)" and "Offense (Intercept and Exploit Foreign Signals)," one top secret NSA document enumerates some of the services supplied by such corporations:



TOP SECRET//COMINT//X1

NSA Strategic Partnerships

Alliances with over 80 Major Global Corporations Supporting both Missions

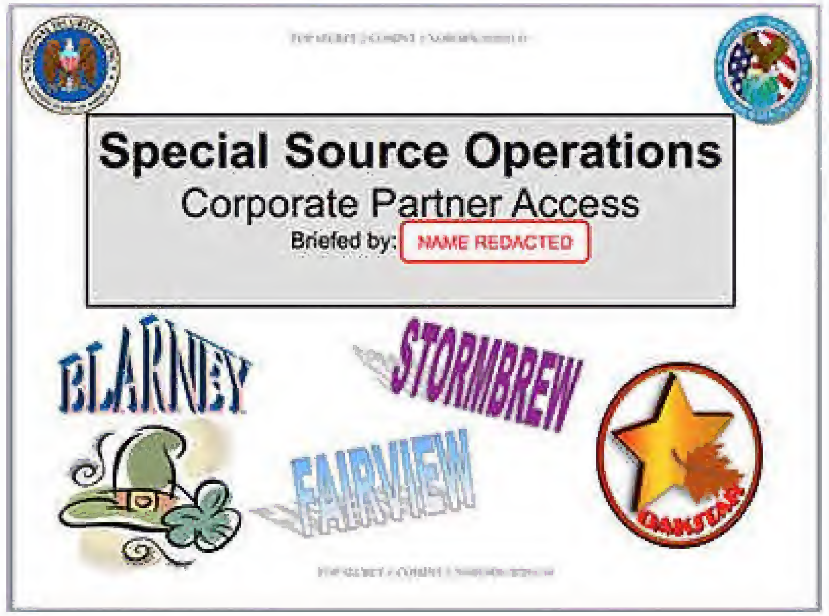
- Telecommunications & Network Service Providers
- Network Infrastructure
- Hardware Platforms Desktops/Servers
- Operating Systems
- Applications Software
- Security Hardware & Software
- System Integrators

AT&T
Qwest
EDS
H-P
Motorola
CISCO
Qualcomm
Oracle
IBM
Intel
Microsoft
Verizon

TOP SECRET//COMINT//X1

These corporate partnerships, which provide the systems and the access on which the NSA depends, are managed by the NSA's highly secret Special Sources Operations unit, the division that oversees corporate partnerships. Snowden described the SSO as the "crown jewel" of the organization.

BLARNEY, FAIRVIEW, OAKSTAR, and STORMBREW are some of the programs overseen by the SSO within its Corporate Partner Access (CPA) portfolio.



Special Source Operations

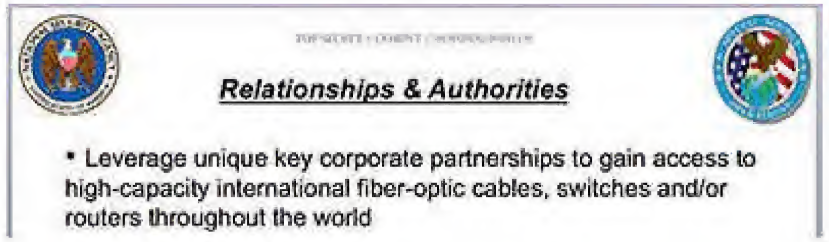
Corporate Partner Access

Briefed by: NAME REDACTED

BLARNEY
STORMBREW
FAIRVIEW
OAKSTAR

As part of these programs, the NSA exploits the access that certain telecom companies have to international systems, having entered into contracts with foreign telecoms to build, maintain, and upgrade their networks. The US companies then redirect the target country's communications data to NSA repositories.

The core purpose of BLARNEY is depicted in one NSA briefing:

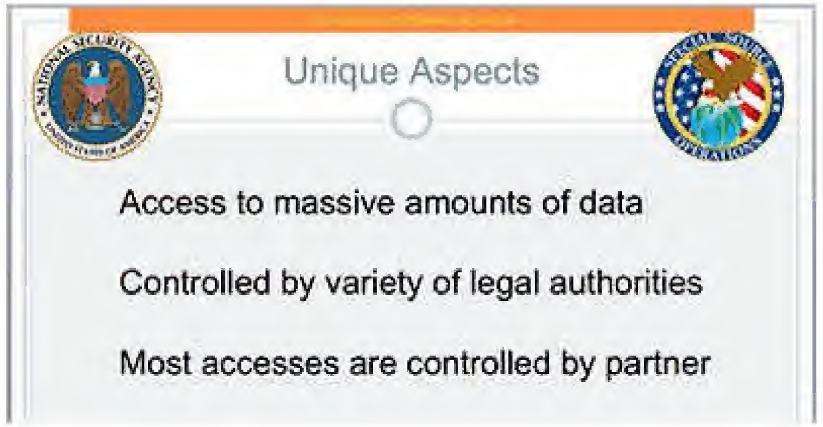


Relationships & Authorities

- Leverage unique key corporate partnerships to gain access to high-capacity international fiber-optic cables, switches and/or routers throughout the world

BLARNEY relied on one relationship in particular—a long-standing partnership with AT&T Inc., according to the *Wall Street Journal*'s reporting on the program. According to the NSA's own files, in 2010 the list of countries targeted by BLARNEY included Brazil, France, Germany, Greece, Israel, Italy, Japan, Mexico, South Korea, and Venezuela, as well as the European Union and the United Nations.

FAIRVIEW, another SSO program, also collects what the NSA touts as "massive amounts of data" from around the world. And it, too, relies mostly on a single "corporate partner" and, in particular, that partner's access to the telecommunications systems of foreign nations. The NSA's internal summary of FAIRVIEW is simple and clear:

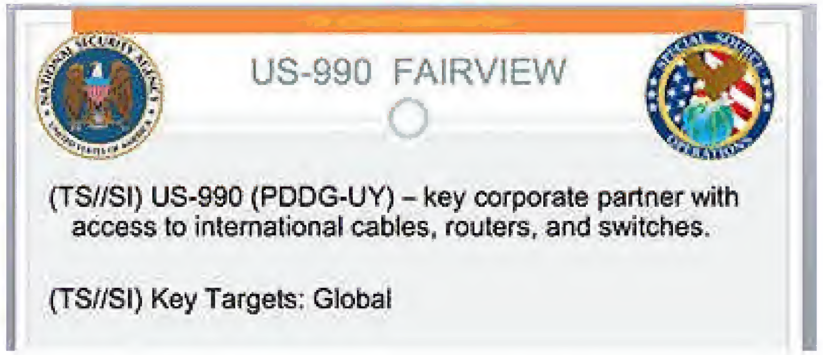


Unique Aspects

Access to massive amounts of data

Controlled by variety of legal authorities

Most accesses are controlled by partner

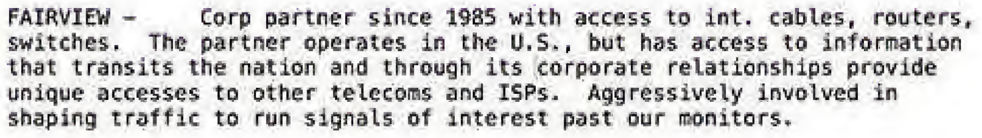


US-990 FAIRVIEW

(TS//SI) US-990 (PDDG-UY) – key corporate partner with access to international cables, routers, and switches.

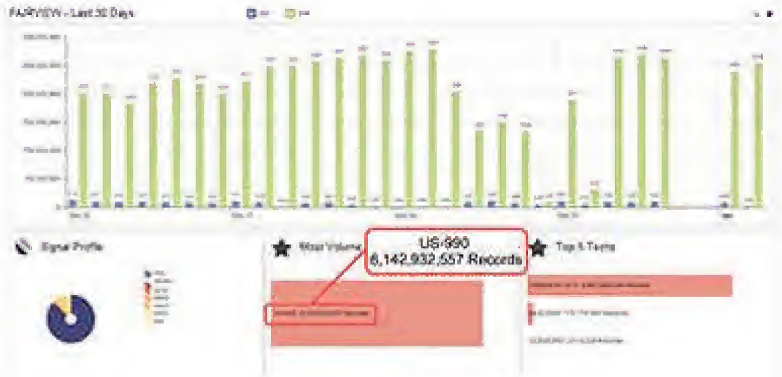
(TS//SI) Key Targets: Global

According to NSA documents, FAIRVIEW "is typically in the top five at NSA as a collection source for serialized production"—meaning ongoing surveillance—"and one of the largest providers of metadata." Its overwhelming reliance on one telecom is demonstrated by its claim that "approximately 75% of reporting is single source, reflecting the unique access the program enjoys to a wide variety of target communications." Though the telecom is not identified, one description of the FAIRVIEW partner makes clear its eagerness to cooperate:

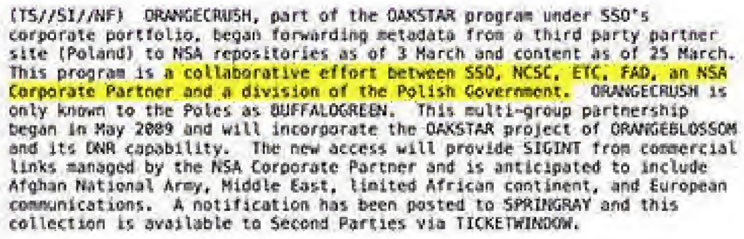


```
FAIRVIEW -     Corp partner since 1985 with access to int. cables, routers,
switches.  The partner operates in the U.S., but has access to information
that transits the nation and through its corporate relationships provide
unique accesses to other telecoms and ISPs.  Aggressively involved in
shaping traffic to run signals of interest past our monitors.
```

Thanks to such cooperation, the FAIRVIEW program collects vast quantities of information about telephone calls. One chart, which covers the thirty-day period beginning December 10, 2012, shows that just this program alone was responsible for the collection of some two hundred million records each day that month, for a thirty-day total of more than six billion records. The light bars are collections of "DNR" (telephone calls), while the dark bars are "DNI" (Internet activity):

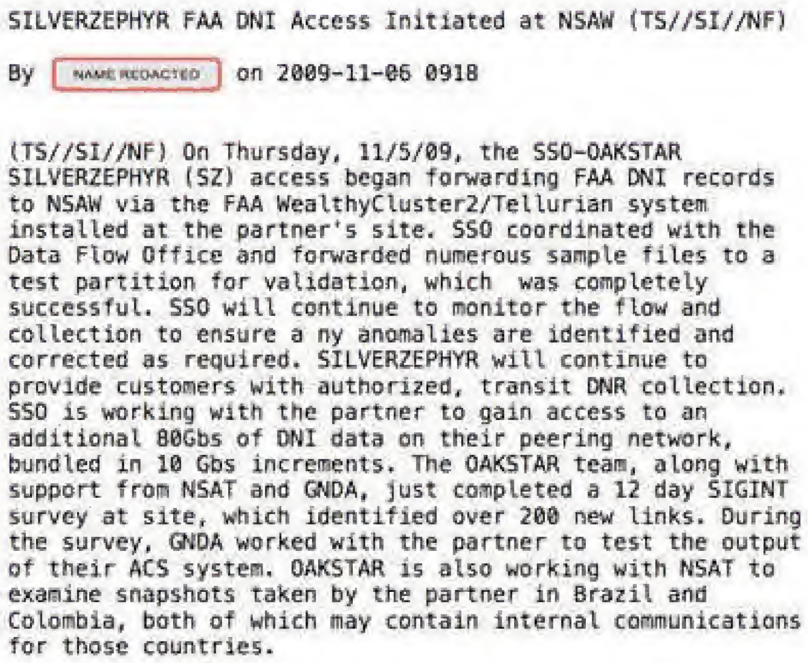


To collect these billions of phone records, the SSO collaborates with the NSA's corporate partners as well as with foreign government agencies—for instance, the Polish intelligence service:



```
(TS//SI//NF)  ORANGECRUSH, part of the OAKSTAR program under SSO's
corporate portfolio, began forwarding metadata from a third party partner
site (Poland) to NSA repositories as of 3 March and content as of 25 March.
This program is a collaborative effort between SSO, NCSC, ETC, FAD, an NSA
Corporate Partner and a division of the Polish Government.  ORANGECRUSH is
only known to the Poles as BUFFALOGREEN.  This multi-group partnership
began in May 2009 and will incorporate the OAKSTAR project of ORANGEBLOSSOM
and its DNR capability.  The new access will provide SIGINT from commercial
links managed by the NSA Corporate Partner and is anticipated to include
Afghan National Army, Middle East, limited African continent, and European
communications.  A notification has been posted to SPRINGRAY and this
collection is available to Second Parties via TICKETWINDOW.
```

The OAKSTAR program similarly exploits the access that one of the NSA's corporate partners (code-named STEELKNIGHT) has to foreign telecommunications systems, using that access to redirect data into the NSA's own repositories. Another partner, code-named SILVERZEPHYR, appears in a November 11, 2009, document describing work done with the company to obtain "internal communications" from both Brazil and Colombia:

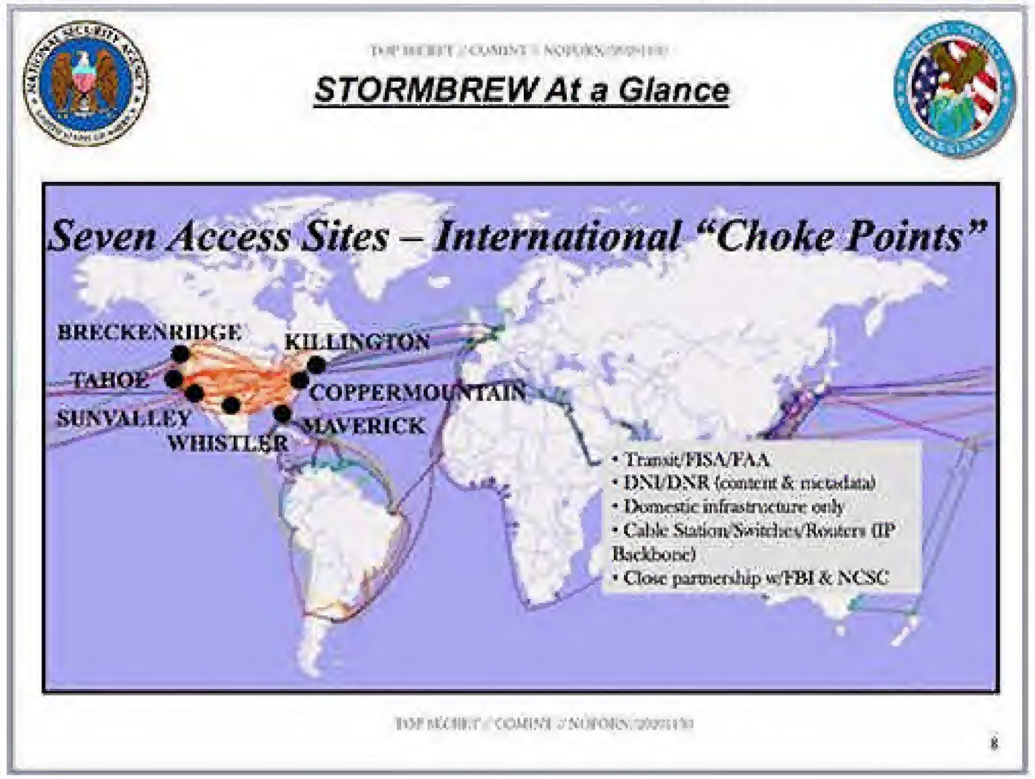


```
SILVERZEPHYR FAA DNI Access Initiated at NSAW (TS//SI//NF)

By NAME REDACTED on 2009-11-06 0918

(TS//SI//NF) On Thursday, 11/5/09, the SSO-OAKSTAR
SILVERZEPHYR (SZ) access began forwarding FAA DNI records
to NSAW via the FAA WealthyCluster2/Tellurian system
installed at the partner's site. SSO coordinated with the
Data Flow Office and forwarded numerous sample files to a
test partition for validation, which  was completely
successful. SSO will continue to monitor the flow and
collection to ensure a ny anomalies are identified and
corrected as required. SILVERZEPHYR will continue to
provide customers with authorized, transit DNR collection.
SSO is working with the partner to gain access to an
additional 80Gbs of DNI data on their peering network,
bundled in 10 Gbs increments. The OAKSTAR team, along with
support from NSAT and GNDA, just completed a 12 day SIGINT
survey at site, which identified over 200 new links. During
the survey, GNDA worked with the partner to test the output
of their ACS system. OAKSTAR is also working with NSAT to
examine snapshots taken by the partner in Brazil and
Colombia, both of which may contain internal communications
for those countries.
```

Meanwhile, the STORMBREW program, conducted in "close partnership with the FBI," gives the NSA access to Internet and telephone traffic that enters the United States at various "choke points" on US soil. It exploits the fact that the vast majority of the world's Internet traffic at some point flows through the US communications infrastructure—a residual by-product of the central role that the United States had played in developing the network. Some of these designated choke points are identified by cover names:



TOP SECRET // COMINT // NOFORN//20291130

STORMBREW At a Glance

Seven Access Sites – International "Choke Points"

- Transit/FISA/FAA
- DNI/DNR (content & metadata)
- Domestic infrastructure only
- Cable Station/Switches/Routers (IP Backbone)
- Close partnership w/FBI & NCSC

TOP SECRET // COMINT // NOFORN//20291130

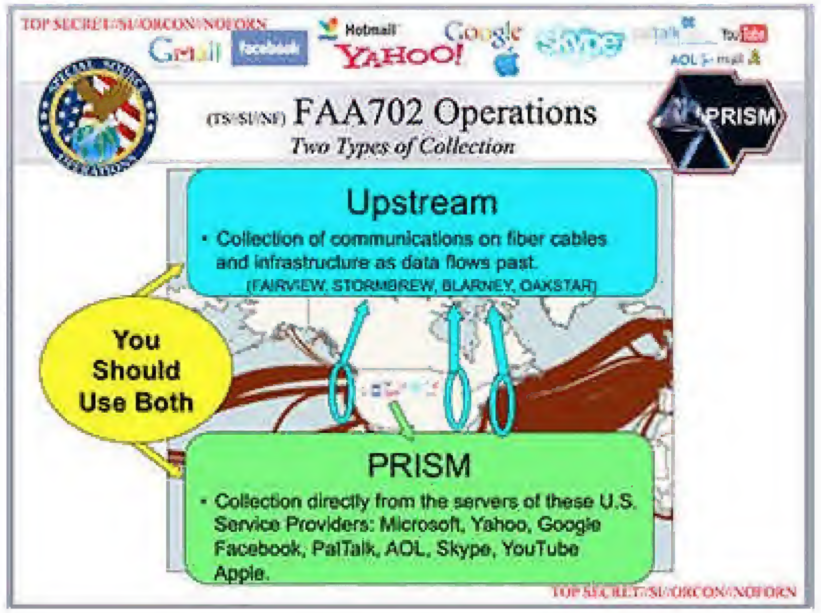
8

According to the NSA, STORMBREW "is currently comprised of very sensitive relationships with two U.S. telecom providers (cover terms ARTIFICE and WOLFPOINT)." Beyond its access to US-based choke points, "the STORMBREW program also manages two submarine cable landing access sites; one on the USA west coast (cover term, BRECKENRIDGE), and the other on the USA east coast (cover term QUAIL-CREEK)."

As the profusion of cover names attests, the identity of its corporate partners is one of the most closely guarded secrets in the NSA. The documents containing the key to those code names are vigilantly safeguarded by the agency and Snowden was unable to obtain many of them. Nonetheless, his revelations did unmask some of the companies cooperating with the NSA. Most famously, his archive included the PRISM documents, which detailed secret agreements between the NSA and the world's largest Internet companies—Facebook, Yahoo!, Apple, Google—as well as extensive efforts by

Microsoft to provide the agency with access to its communications platforms such as Outlook.

Unlike BLARNEY, FAIRVIEW, OAKSTAR, and STORMBREW, which entail tapping into fiber-optic cables and other forms of infrastructure ("upstream" surveillance, in NSA parlance), PRISM allows the NSA to collect data directly from the servers of nine of the biggest Internet companies:



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past. (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

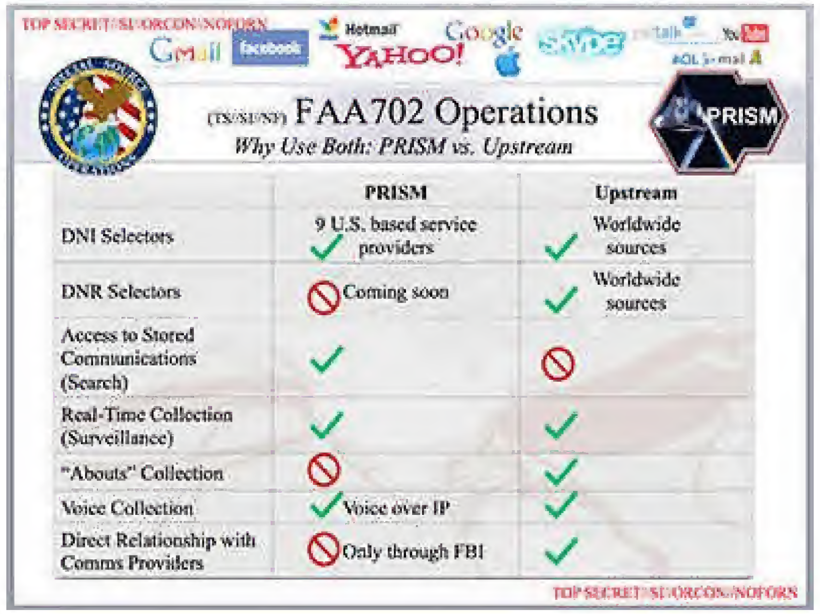
TOP SECRET//SI//ORCON//NOFORN

The companies listed on the PRISM slide denied allowing the NSA unlimited access to their servers. Facebook and Google, for instance, claimed that they only give the NSA information for which the agency has a warrant, and tried to depict PRISM as little more than a trivial technical detail: a slightly upgraded delivery system whereby the NSA receives data in a "lockbox" that the companies are legally compelled to provide.

But their argument is belied by numerous points. For one, we know that Yahoo! vigorously fought in court against the NSA's efforts to force it to join PRISM—an unlikely effort if the program were simply a trivial change to a delivery system. (Yahoo!'s claims were rejected by the FISA court, and the company was ordered to participate in PRISM.) Second, the *Washington Post*'s Bart Gellman, after receiving heavy criticism for "overstating" the impact of PRISM, reinvestigated the program and confirmed that he stood by the *Post*'s central claim: "From their workstations anywhere in the world, government employees cleared for PRISM access may 'task' the system"—that is, run a search—"and receive results from an Internet company without further interaction with the company's staff."

Third, the Internet companies' denials were phrased in evasive and legalistic fashion, often obfuscating more than clarifying. For instance, Facebook claimed not to provide "direct access," while Google denied having created a "back door" for the NSA. But as Chris Soghoian, the ACLU's tech expert, told *Foreign Policy*, these were highly technical terms of art denoting very specific means to get at information. The companies ultimately did not deny that they had worked with the NSA to set up a system through which the agency could directly access their customers' data.

Finally, the NSA itself has repeatedly hailed PRISM for its unique collection capabilities and noted that the program has been vital for increasing surveillance. One NSA slide details PRISM's special surveillance powers:



TOP SECRET//SI//ORCON//NOFORN

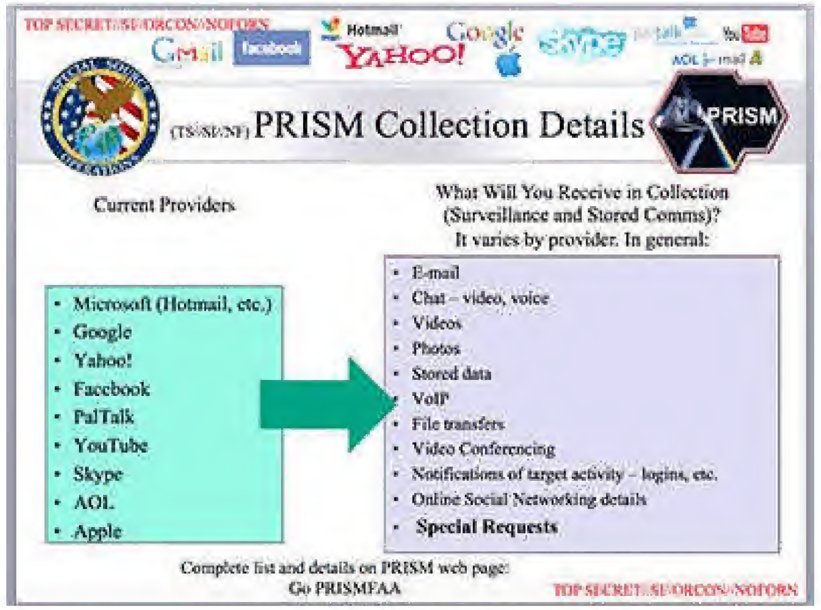
(TS//SI//NF) FAA702 Operations

Why Use Both: PRISM vs. Upstream

	PRISM	Upstream
DNI Selectors	✓ 9 U.S. based service providers	✓ Worldwide sources
DNR Selectors	⊘ Coming soon	✓ Worldwide sources
Access to Stored Communications (Search)	✓	⊘
Real-Time Collection (Surveillance)	✓	✓
"Abouts" Collection	⊘	✓
Voice Collection	✓ Voice over IP	✓
Direct Relationship with Comms Providers	⊘ Only through FBI	✓

TOP SECRET//SI//ORCON//NOFORN

Another details the wide range of communications that PRISM enables the NSA to access:



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

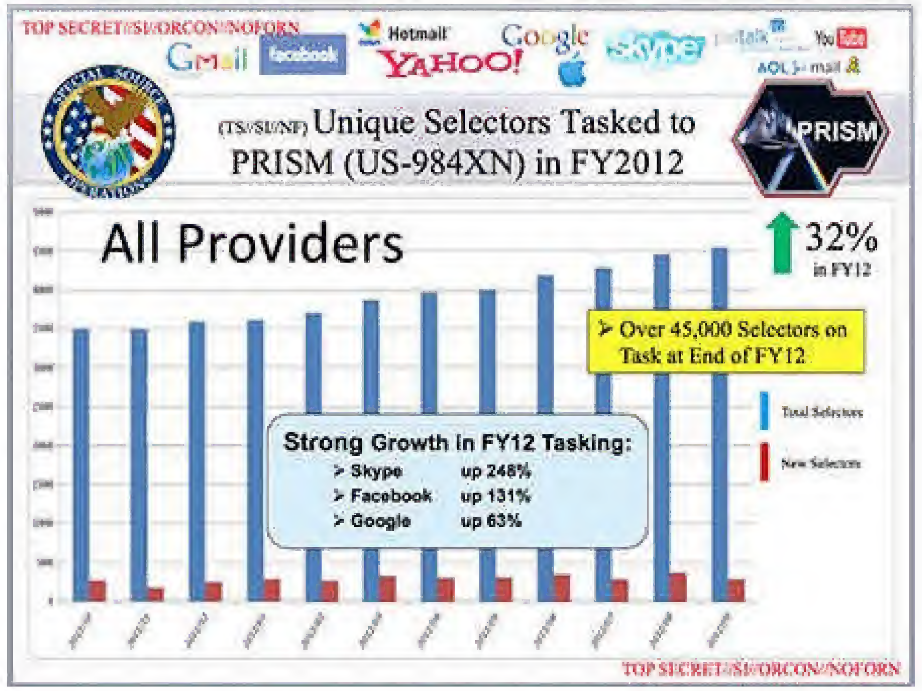
What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

And another NSA slide details how the PRISM program has steadily and substantially increased the agency's collection:



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Unique Selectors Tasked to PRISM (US-984XN) in FY2012

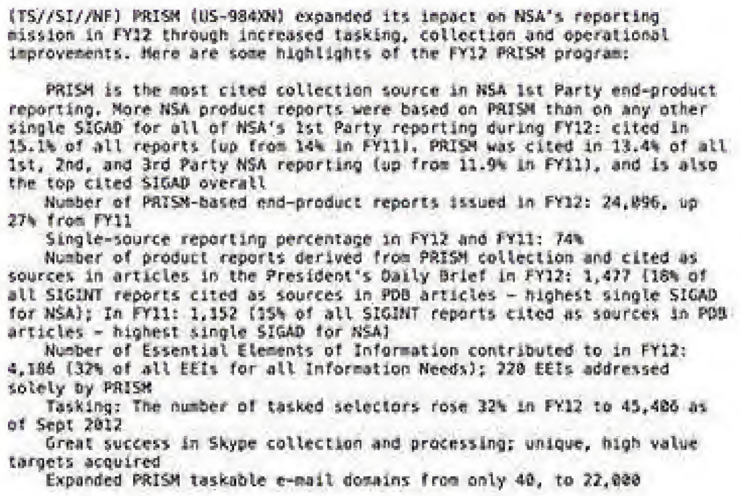
➢ Over 45,000 Selectors on Task at End of FY12

Strong Growth in FY12 Tasking:

➢ Skype up 248%
➢ Facebook up 131%
➢ Google up 63%

TOP SECRET//SI//ORCON//NOFORN

On its internal messaging boards, the Special Source Operation division frequently hails the massive collection value PRISM has provided. One message, from November 19, 2012, is entitled "PRISM Expands Impact: FY12 Metrics":



(TS//SI//NF) PRISM (US-984XN) expanded its impact on NSA's reporting mission in FY12 through increased tasking, collection and operational improvements. Here are some highlights of the FY12 PRISM program:

PRISM is the most cited collection source in NSA 1st Party end-product reporting. More NSA product reports were based on PRISM than on any other single SIGAD for all of NSA's 1st Party reporting during FY12: cited in 15.1% of all reports (up from 14% in FY11). PRISM was cited in 13.4% of all 1st, 2nd, and 3rd Party NSA reporting (up from 11.9% in FY11), and is also the top cited SIGAD overall

Number of PRISM-based end-product reports issued in FY12: 24,096, up 27% from FY11

Single-source reporting percentage in FY12 and FY11: 74%

Number of product reports derived from PRISM collection and cited as sources in articles in the President's Daily Brief in FY12: 1,477 (18% of all SIGINT reports cited as sources in PDB articles – highest single SIGAD for NSA); In FY11: 1,152 (15% of all SIGINT reports cited as sources in PDB articles – highest single SIGAD for NSA)

Number of Essential Elements of Information contributed to in FY12: 4,186 (32% of all EEIs for all Information Needs); 220 EEIs addressed solely by PRISM

Tasking: The number of tasked selectors rose 32% in FY12 to 45,406 as of Sept 2012

Great success in Skype collection and processing; unique, high value targets acquired

Expanded PRISM taskable e-mail domains from only 40, to 22,000

Such congratulatory proclamations do not support the notion of PRISM as only a trivial technicality, and they give the lie to Silicon Valley's denials of cooperation. Indeed, the *New York Times*, reporting on the PRISM program after Snowden's revelations, described a slew of secret negotiations between the NSA and Silicon Valley about providing the agency with unfettered access to the companies' systems. "When government officials came to Silicon Valley to demand easier ways for the world's largest Internet companies to turn over user data as part of a secret surveillance program, the companies bristled," reported the *Times*. "In the end, though, many cooperated at least a bit." In particular:

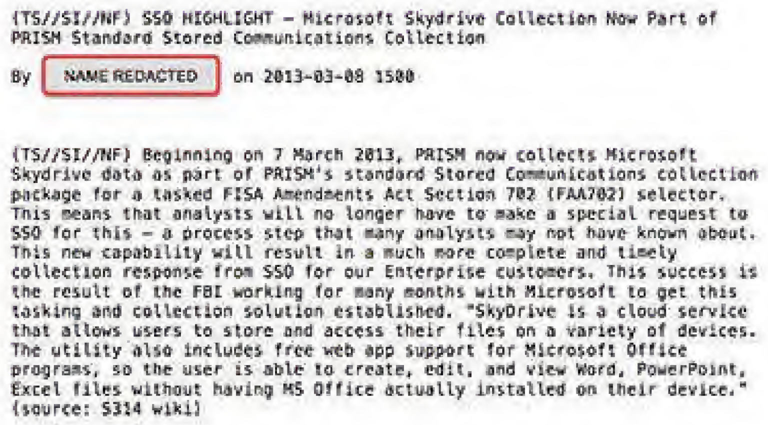
> Twitter declined to make it easier for the government. But other companies were more compliant, according to people briefed on the negotiations. They opened discussions with national security officials about developing technical methods to more efficiently and securely share the personal data of foreign users in response to lawful government requests. And in some cases, they changed their computer systems to do so.

These negotiations, the *New York Times* said, "illustrate how intricately the government and tech companies work together, and the depth of their behind-the-scenes transactions." The article also contested the companies' claims that they provide the NSA only with access that is legally compelled, noting: "While handing over data in response to a legitimate FISA request is a legal requirement, making it easier for the government to get the information is not, which is why Twitter could decline to do so."

The Internet companies' claim that they hand over to the NSA just the information that they are legally required to provide is also not particularly meaningful. That's because the NSA only needs to obtain an individual warrant when it wants to specifically target a US person. No such special permission is required for the agency to obtain the communications data of any non-American on foreign soil, *even when that person is communicating with Americans*. Similarly, there is no check or limit on the NSA's bulk collection of metadata, thanks to the government's interpretation of the Patriot Act—an interpretation so broad that even the law's original authors were shocked to learn how it was being used.

The close collaboration between the NSA and private corporations is perhaps best seen in the documents relating to Microsoft, which reveal the company's vigorous efforts to give the NSA access to several of its most used online services, including SkyDrive, Skype, and Outlook.com.

SkyDrive, which allows people to store their files online and access them from various devices, has more than 250 million users worldwide. "We believe it's important that you have control over who can and cannot access your personal data in the cloud," Microsoft's SkyDrive website proclaims. Yet as an NSA document details, Microsoft spent "many months" working to provide the government with easier access to that data:

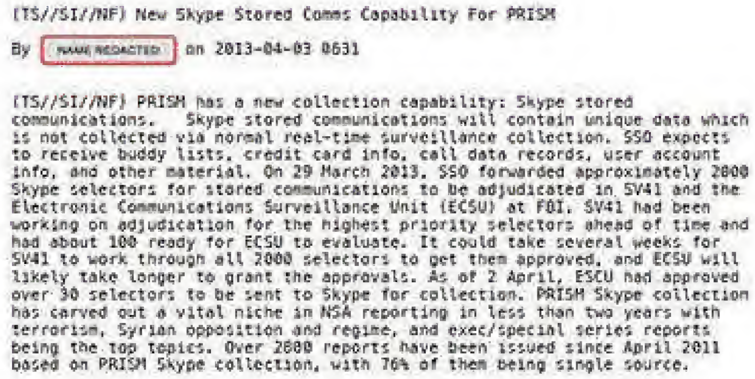


(TS//SI//NF) SSO HIGHLIGHT – Microsoft Skydrive Collection Now Part of PRISM Standard Stored Communications Collection

By NAME REDACTED on 2013-03-08 1500

(TS//SI//NF) Beginning on 7 March 2013, PRISM now collects Microsoft Skydrive data as part of PRISM's standard Stored Communications collection package for a tasked FISA Amendments Act Section 702 (FAA702) selector. This means that analysts will no longer have to make a special request to SSO for this – a process step that many analysts may not have known about. This new capability will result in a much more complete and timely collection response from SSO for our Enterprise customers. This success is the result of the FBI working for many months with Microsoft to get this tasking and collection solution established. "SkyDrive is a cloud service that allows users to store and access their files on a variety of devices. The utility also includes free web app support for Microsoft Office programs, so the user is able to create, edit, and view Word, PowerPoint, Excel files without having MS Office actually installed on their device." (source: S314 wiki)

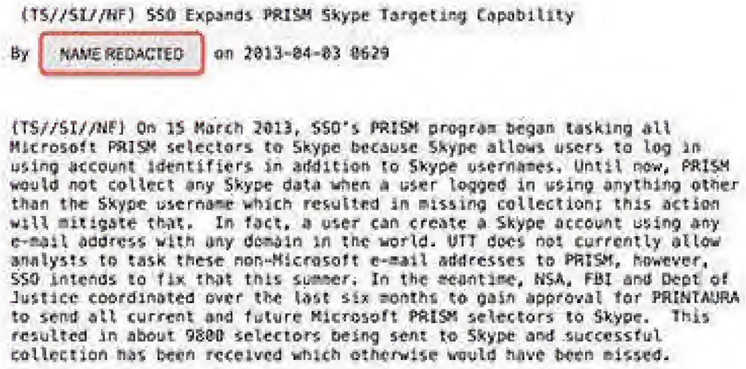
In late 2011, Microsoft purchased Skype, the Internet-based telephone and chat service with over 663 million registered users. At the time of its purchase, Microsoft assured users that "Skype is committed to respecting your privacy and the confidentiality of your personal data, traffic, and communications content." But in fact, this data, too, was readily available to the government. By early 2013, there were multiple messages on the NSA system celebrating the agency's steadily improving access to the communications of Skype users:



(TS//SI//NF) New Skype Stored Comms Capability For PRISM

By NAME REDACTED on 2013-04-03 0631

(TS//SI//NF) PRISM has a new collection capability: Skype stored communications. Skype stored communications will contain unique data which is not collected via normal real-time surveillance collection. SSO expects to receive buddy lists, credit card info, call data records, user account info, and other material. On 29 March 2013, SSO forwarded approximately 2000 Skype selectors for stored communications to be adjudicated in SV41 and the Electronic Communications Surveillance Unit (ECSU) at FBI. SV41 had been working on adjudication for the highest priority selectors ahead of time and had about 100 ready for ECSU to evaluate. It could take several weeks for SV41 to work through all 2000 selectors to get them approved, and ECSU will likely take longer to grant the approvals. As of 2 April, ESCU had approved over 30 selectors to be sent to Skype for collection. PRISM Skype collection has carved out a vital niche in NSA reporting in less than two years with terrorism, Syrian opposition and regime, and exec/special series reports being the top topics. Over 2000 reports have been issued since April 2011 based on PRISM Skype collection, with 76% of them being single source.



(TS//SI//NF) SSO Expands PRISM Skype Targeting Capability

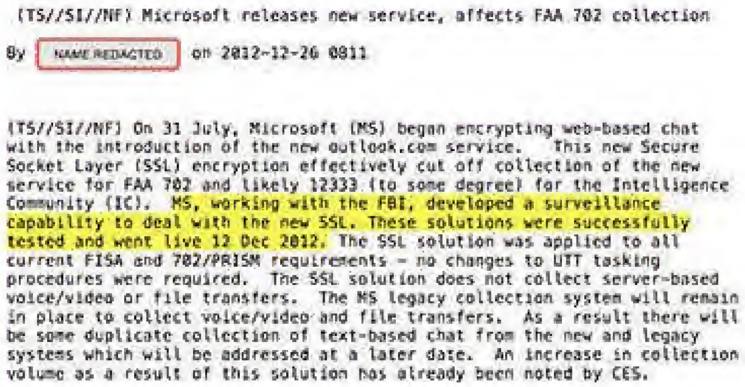
By NAME REDACTED on 2013-04-03 0629

(TS//SI//NF) On 15 March 2013, SSO's PRISM program began tasking all Microsoft PRISM selectors to Skype because Skype allows users to log in using account identifiers in addition to Skype usernames. Until now, PRISM would not collect any Skype data when a user logged in using anything other than the Skype username which resulted in missing collection; this action will mitigate that. In fact, a user can create a Skype account using any e-mail address with any domain in the world. UTT does not currently allow analysts to task these non-Microsoft e-mail addresses to PRISM, however, SSO intends to fix that this summer. In the meantime, NSA, FBI and Dept of Justice coordinated over the last six months to gain approval for PRINTAURA to send all current and future Microsoft PRISM selectors to Skype. This resulted in about 9800 selectors being sent to Skype and successful collection has been received which otherwise would have been missed.

Not only was all this collaboration conducted with no transparency, but it contradicted public statements made by Skype. ACLU technology expert Chris Soghoian said the revelations would surprise many Skype customers. "In the past, Skype made affirmative promises to users about their inability to perform wiretaps," he said. "It's hard to square Microsoft's secret collaboration with the NSA with its high-profile efforts to compete on privacy with Google."

In 2012, Microsoft began upgrading its email portal, Outlook.com, to merge all of its communications services—including the widely used Hotmail—into one central program. The company touted the new Outlook by promising high levels of encryption to protect privacy, and the NSA quickly grew concerned that the encryption Microsoft offered to Outlook customers would block the agency from spying on their communications. One SSO memo from August 22, 2012, frets that "using this portal means that email emerging from it will be encrypted with the default setting" and that "chat sessions conducted within the portal are also encrypted when both communicants are using a Microsoft encrypted chat client."

But that worry was short-lived. Within a few months, the two entities got together and devised methods for the NSA to circumvent the very encryption protections Microsoft was publicly advertising as vital for protecting privacy:



(TS//SI//NF) Microsoft releases new service, affects FAA 702 collection

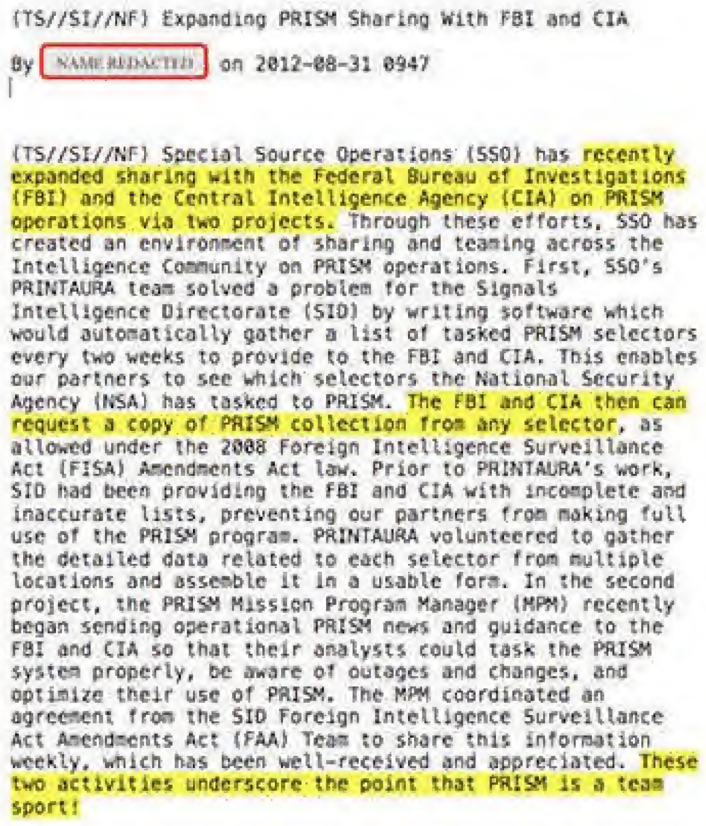
By NAME REDACTED on 2012-12-26 0811

(TS//SI//NF) On 31 July, Microsoft (MS) began encrypting web-based chat with the introduction of the new outlook.com service. This new Secure Socket Layer (SSL) encryption effectively cut off collection of the new service for FAA 702 and likely 12333 (to some degree) for the Intelligence Community (IC). MS, working with the FBI, developed a surveillance capability to deal with the new SSL. These solutions were successfully tested and went live 12 Dec 2012. The SSL solution was applied to all current FISA and 702/PRISM requirements - no changes to UTT tasking procedures were required. The SSL solution does not collect server-based voice/video or file transfers. The MS legacy collection system will remain in place to collect voice/video and file transfers. As a result there will be some duplicate collection of text-based chat from the new and legacy systems which will be addressed at a later date. An increase in collection volume as a result of this solution has already been noted by CES.

Another document describes further collaboration between Microsoft and the FBI, as that agency also sought to ensure that new Outlook features did not interfere with its surveillance habits: "The FBI Data Intercept Technology Unit

(DITU) team is working with Microsoft to understand an additional feature in Outlook.com which allows users to create email aliases, which may affect our tasking process.... There are compartmented and other activities underway to mitigate these problems."

Finding this mention of FBI surveillance in Snowden's archive of internal NSA documents was not an isolated occurrence. The entire intelligence community is able to access the information that the NSA collects: it routinely shares its vast trove of data with other agencies, including the FBI and the CIA. One principal purpose of the NSA's great spree of data collection was precisely to boost the spread of information across the board. Indeed, almost every document pertaining to the various collection programs mentions the inclusion of other intelligence units. This 2012 entry from the NSA's SSO unit, on sharing PRISM data, gleefully declares that "PRISM is a team sport!":



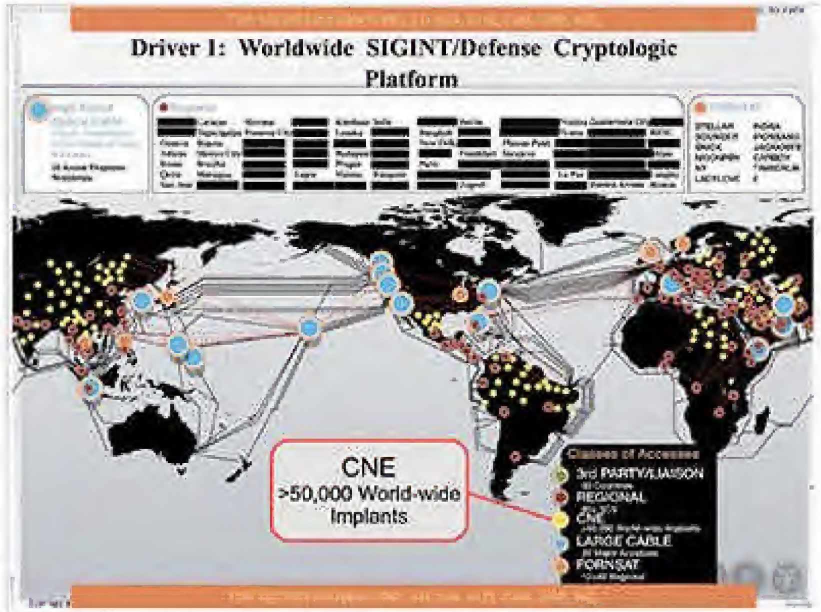
(TS//SI//NF) Expanding PRISM Sharing With FBI and CIA

By NAME REDACTED on 2012-08-31 0947

(TS//SI//NF) Special Source Operations (SSO) has recently expanded sharing with the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA) on PRISM operations via two projects. Through these efforts, SSO has created an environment of sharing and teaming across the Intelligence Community on PRISM operations. First, SSO's PRINTAURA team solved a problem for the Signals Intelligence Directorate (SID) by writing software which would automatically gather a list of tasked PRISM selectors every two weeks to provide to the FBI and CIA. This enables our partners to see which selectors the National Security Agency (NSA) has tasked to PRISM. The FBI and CIA then can request a copy of PRISM collection from any selector, as allowed under the 2008 Foreign Intelligence Surveillance Act (FISA) Amendments Act law. Prior to PRINTAURA's work, SID had been providing the FBI and CIA with incomplete and inaccurate lists, preventing our partners from making full use of the PRISM program. PRINTAURA volunteered to gather the detailed data related to each selector from multiple locations and assemble it in a usable form. In the second project, the PRISM Mission Program Manager (MPM) recently began sending operational PRISM news and guidance to the FBI and CIA so that their analysts could task the PRISM system properly, be aware of outages and changes, and optimize their use of PRISM. The MPM coordinated an agreement from the SID Foreign Intelligence Surveillance Act Amendments Act (FAA) Team to share this information weekly, which has been well-received and appreciated. These two activities underscore the point that PRISM is a team sport!

"Upstream" collection (from fiber-optic cables) and direct collection from the servers of Internet companies (PRISM) account for most of the records gathered by the NSA. In addition to such sweeping surveillance, though, the NSA also carries out what it calls Computer Network Exploitation (CNE), placing malware in individual computers to surveil their users. When the agency succeeds in inserting such malware, it is able, in NSA terminology, to "own" the computer: to view every keystroke entered and every screen viewed. The Tailored Access Operations (TAO) division responsible for this work is, in effect, the agency's own private hacker unit.

The hacking practice is quite widespread in its own right: one NSA document indicates that the agency has succeeded in infecting at least fifty thousand individual computers with a type of malware called "Quantum Insertion." One map shows the places where such operations have been performed and the number of successful insertions:


Driver 1: Worldwide SIGINT/Defense Cryptologic Platform
[redacted]
CNE
>50,000 World-wide Implants
Classes of Accesses
3rd PARTY/LIAISON
REGIONAL
CNE
LARGE CABLE
FORNSAT

Using Snowden documents, the *New York Times* reported that the NSA has in fact implanted this particular software "in nearly 100,000 computers around the world." Although the malware is usually installed by "gaining access to computer networks, the NSA has increasingly made use of a secret technology that enables it to enter and alter data in computers even if they are not connected to the Internet."

* * *

Beyond its work with compliant telecoms and Internet companies, the NSA has also colluded with foreign governments to construct its far-reaching surveillance system. Broadly speaking, the NSA has three different categories of foreign relationships. The first is with the Five Eyes group: the US spies with these countries, but rarely on them, unless requested to by those countries' own officials. The second tier involves countries that the NSA works with for specific surveillance projects while also spying on them extensively. The third group is comprised of countries on which the United States routinely spies but with whom it virtually never cooperates.

Within the Five Eyes group, the closest NSA ally is the British GCHQ. As the *Guardian* reported, based on documents provided by Snowden, "The U.S. government has paid at least £100m to the UK spy agency GCHQ over the last three years to secure access to and influence over Britain's intelligence gathering programs." Those payments were an incentive to GCHQ to support the NSA's surveillance agenda. "GCHQ must pull its weight and be seen to pull its weight," a secret GCHQ strategy briefing said.

The Five Eyes members share most of their surveillance activities and meet each year at a Signals Development conference, where they boast of their expansion and the prior year's successes. Former NSA deputy director John Inglis has said of the Five Eyes alliance that they "practice intelligence in many regards in a combined way—essentially make sure that we leverage one another's capabilities for mutual benefit."

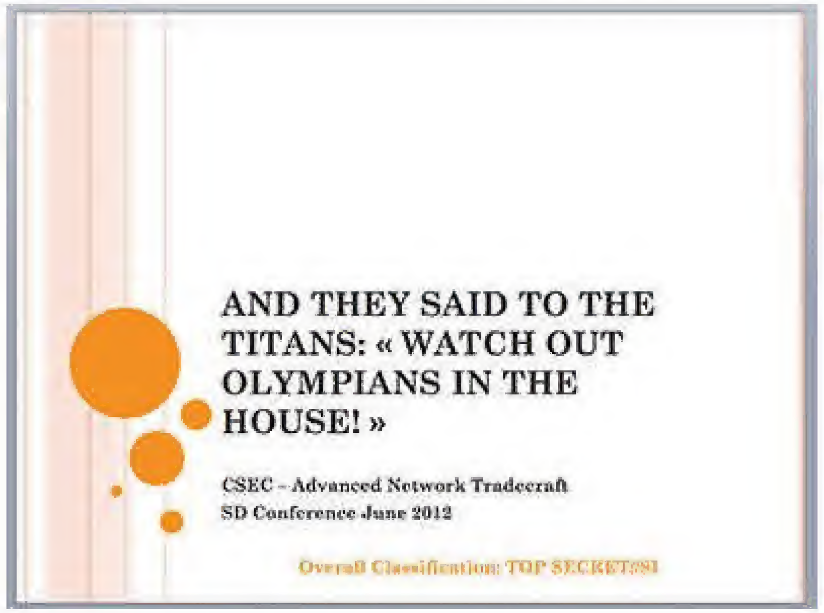
Many of the most invasive surveillance programs are carried out by the Five Eyes partners, a substantial number of these involving the GCHQ. Of special note are the British agency's joint efforts with the NSA to break the common encryption techniques that are used to safeguard personal Internet transactions, such as online banking and retrieval of medical records. The two agencies' success in setting up backdoor access to those encryption systems not only allowed them to peer at people's private dealings, but also weakened the systems for everyone, making them more vulnerable to malicious hackers and to other foreign intelligence agencies.

The GCHQ has also conducted mass interception of communications data from the world's underwater fiber-optic cables. Under the program name Tempora, the GCHQ developed the "ability to tap into and store huge volumes of data drawn from fibre-optic cables for up to 30 days so that it can be sifted and analysed," the *Guardian* reported, and the "GCHQ and the NSA are consequently able to access and process vast quantities of communications between entirely innocent people." The intercepted data encompass all forms of online activity, including "recordings of phone calls, the content of email messages, entries on Facebook, and the history of any internet user's access to websites."

The GCHQ's surveillance activities are every bit as comprehensive—and unaccountable—as the NSA's. As the *Guardian* noted:

> The sheer scale of the agency's ambition is reflected in the titles of its two principal components: Mastering the Internet and Global Telecoms Exploitation, aimed at scooping up as much online and telephone traffic as possible. This is all being carried out without any form of public acknowledgement or debate.

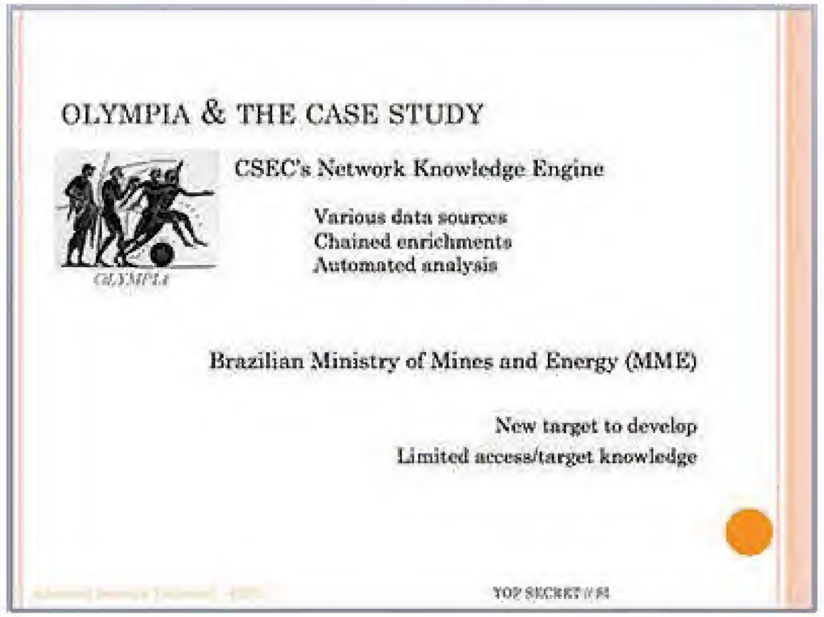
Canada is also a very active partner with the NSA and an energetic surveillance force in its own right. At the 2012 SigDev conference, the Communications Services Establishment Canada (CSEC) boasted about targeting the Brazilian Ministry of Mines and Energy, the agency in Brazil that regulates the industry of greatest interest to Canadian companies:



AND THEY SAID TO THE TITANS: « WATCH OUT OLYMPIANS IN THE HOUSE! »

CSEC – Advanced Network Tradecraft
SD Conference June 2012

Overall Classification: TOP SECRET//SI



OLYMPIA & THE CASE STUDY

CSEC's Network Knowledge Engine

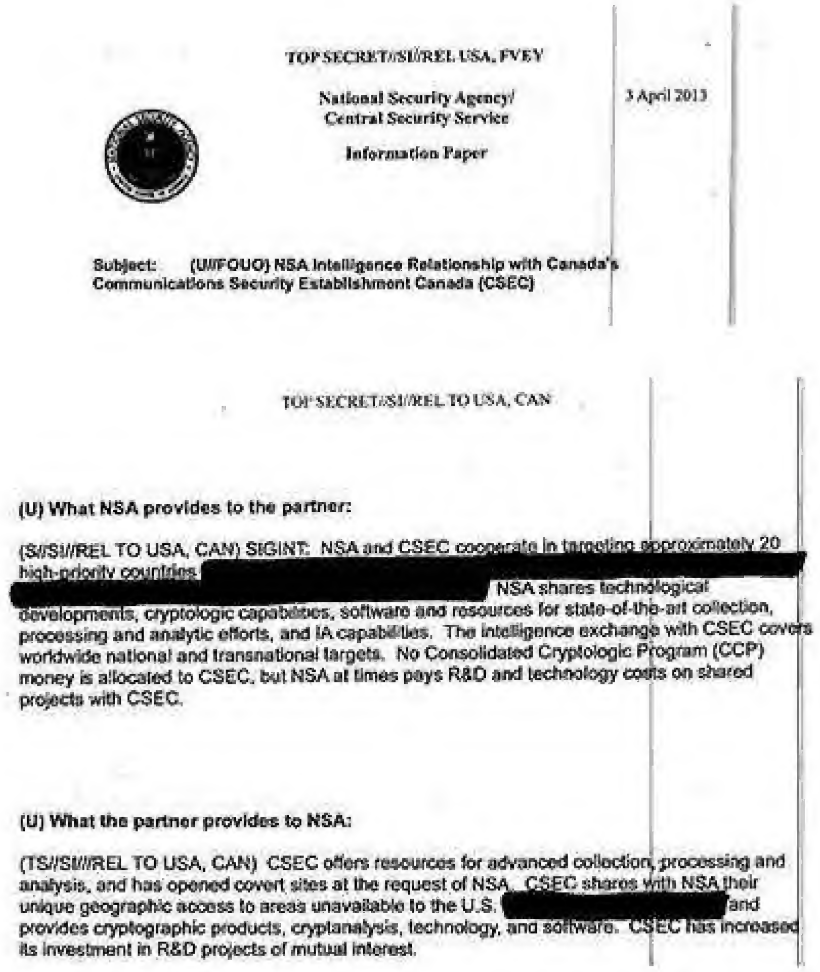
Various data sources
Chained enrichments
Automated analysis

Brazilian Ministry of Mines and Energy (MME)

New target to develop
Limited access/target knowledge

TOP SECRET // SI

There is evidence of widespread CSEC/NSA cooperation, including Canada's efforts to set up spying posts for communications surveillance around the world at the behest and for the benefit of the NSA, and spying on trading partners targeted by the US agency.



TOP SECRET//SI//REL USA, FVEY

National Security Agency/
Central Security Service

Information Paper

3 April 2013

Subject: (U//FOUO) NSA Intelligence Relationship with Canada's Communications Security Establishment Canada (CSEC)

TOP SECRET//SI//REL TO USA, CAN

(U) What NSA provides to the partner:

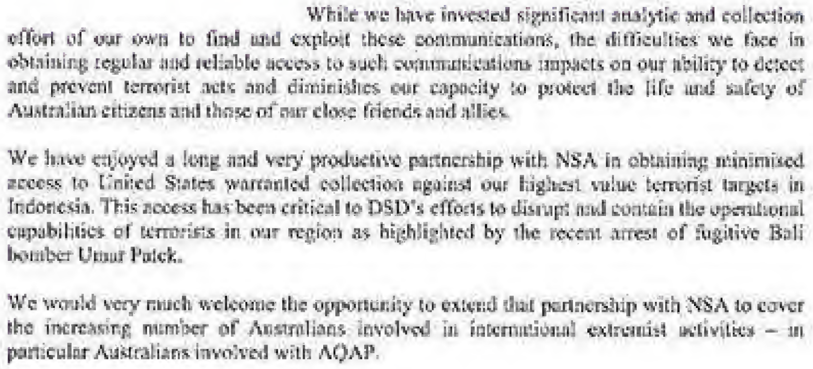
(S//SI//REL TO USA, CAN) SIGINT: NSA and CSEC cooperate in targeting approximately 20 high-priority countries [redacted] NSA shares technological developments, cryptologic capabilities, software and resources for state-of-the-art collection, processing and analytic efforts, and IA capabilities. The intelligence exchange with CSEC covers worldwide national and transnational targets. No Consolidated Cryptologic Program (CCP) money is allocated to CSEC, but NSA at times pays R&D and technology costs on shared projects with CSEC.

(U) What the partner provides to NSA:

(TS//SI//REL TO USA, CAN) CSEC offers resources for advanced collection, processing and analysis, and has opened covert sites at the request of NSA. CSEC shares with NSA their unique geographic access to areas unavailable to the U.S. [redacted] and provides cryptographic products, cryptanalysis, technology, and software. CSEC has increased its investment in R&D projects of mutual interest.

The Five Eyes relationship is so close that member governments place the NSA's desires above the privacy of their own citizens. The *Guardian* reported on one 2007 memo, for instance, describing an agreement "that allowed the agency to 'unmask' and hold on to personal data about Britons that had previously been off limits." Additionally, the rules were changed in 2007 "to allow the NSA to analyse and retain any British citizens' mobile phone and fax numbers, emails and IP addresses swept up by its dragnet."

Going a step further, in 2011 the Australian government explicitly pleaded with the NSA to "extend" their partnership and subject Australian citizens to greater surveillance. In a February 21 letter, the acting deputy director of Australia's Intelligence Defence Signals Directorate wrote to the NSA's Signals Intelligence Directorate, claiming that Australia "now face[s] a sinister and determined threat from 'home grown' extremists active both abroad and within Australia." He requested increased surveillance on the communications of Australian citizens deemed suspicious by their government:

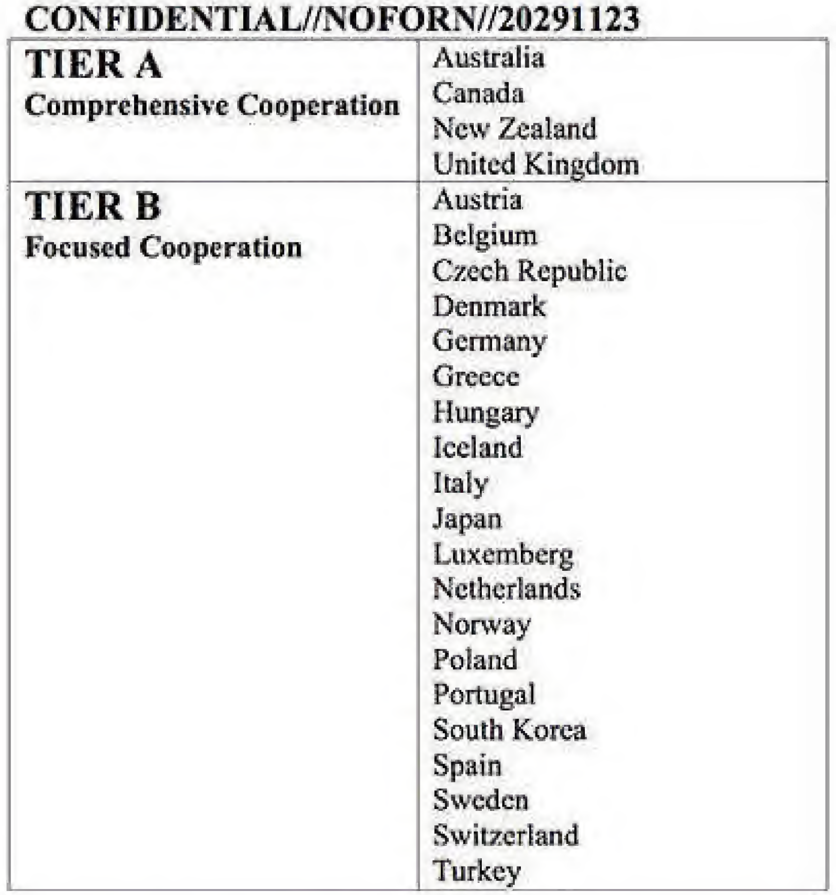


While we have invested significant analytic and collection effort of our own to find and exploit these communications, the difficulties we face in obtaining regular and reliable access to such communications impacts on our ability to detect and prevent terrorist acts and diminishes our capacity to protect the life and safety of Australian citizens and those of our close friends and allies.

We have enjoyed a long and very productive partnership with NSA in obtaining minimised access to United States warranted collection against our highest value terrorist targets in Indonesia. This access has been critical to DSD's effects to disrupt and contain the operational capabilities of terrorists in our region as highlighted by the recent arrest of fugitive Bali bomber Umar Patek.

We would very much welcome the opportunity to extend that partnership with NSA to cover the increasing number of Australians involved in international extremist activities – in particular Australians involved with AQAP.

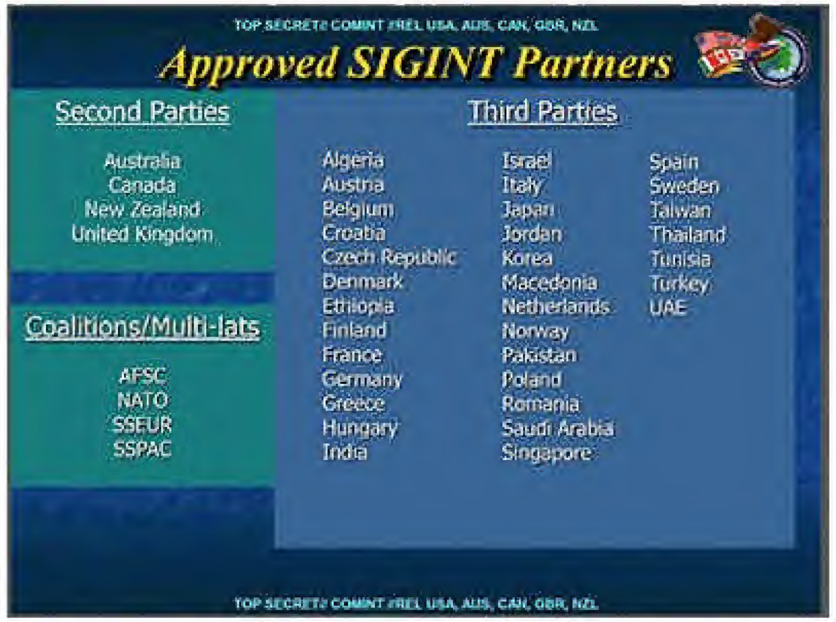
Beyond the Five Eyes partners, the NSA's next level of cooperation is with its Tier B allies: countries that have some limited cooperation with the agency and are also targeted themselves for aggressive, unrequested surveillance. The NSA has clearly delineated these two levels of alliances:



CONFIDENTIAL//NOFORN//20291123

TIER A **Comprehensive Cooperation**	Australia Canada New Zealand United Kingdom
TIER B **Focused Cooperation**	Austria Belgium Czech Republic Denmark Germany Greece Hungary Iceland Italy Japan Luxemberg Netherlands Norway Poland Portugal South Korea Spain Sweden Switzerland Turkey

Using different designations (referring to Tier B as Third Parties), a more recent NSA document—from the Fiscal Year 2013 "Foreign Partner Review"—shows an expanding list of NSA partners, including international organizations such as NATO:



TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

Approved SIGINT Partners

Second Parties

Australia
Canada
New Zealand
United Kingdom

Coalitions/Multi-lats

AFSC
NATO
SSEUR
SSPAC

Third Parties

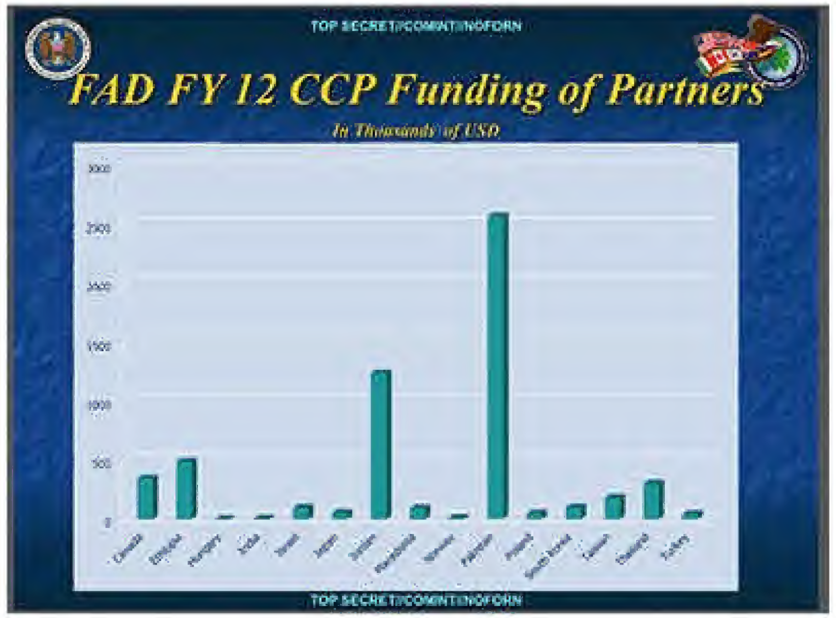
Algeria
Austria
Belgium
Croatia
Czech Republic
Denmark
Ethiopia
Finland
France
Germany
Greece
Hungary
India

Israel
Italy
Japan
Jordan
Korea
Macedonia
Netherlands
Norway
Pakistan
Poland
Romania
Saudi Arabia
Singapore

Spain
Sweden
Taiwan
Thailand
Tunisia
Turkey
UAE

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

As with the GCHQ, the NSA often maintains these partnerships by paying its partner to develop certain technologies and engage in surveillance, and can thus direct how the spying is carried out. The Fiscal Year 2012 "Foreign Partner Review" reveals numerous countries that have received such payments, including Canada, Israel, Japan, Jordan, Pakistan, Taiwan, and Thailand:



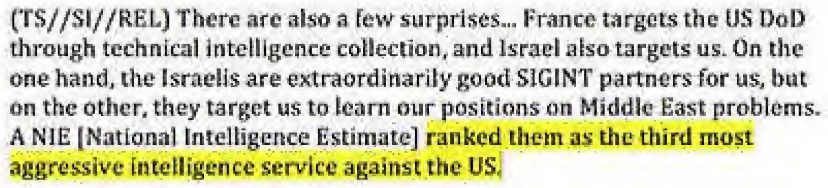
In particular, the NSA has a surveillance relationship with

Israel that often entails cooperation as close as the Five Eyes partnership, if not sometimes even closer. A Memorandum of Understanding between the NSA and the Israeli intelligence service details how the United States takes the unusual step of routinely sharing with Israel raw intelligence containing the communications of American citizens. Among the data furnished to Israel are "unevaluated and unminimized transcripts, gists, facsimiles, telex, voice, and Digital Network Intelligence metadata and content."

What makes this sharing particularly egregious is that the material is sent to Israel without having undergone the legally required process of "minimization." The minimization procedures are supposed to ensure that when the NSA's bulk surveillance sweeps up some communications data that even the agency's very broad guidelines do not permit it to collect, such information is destroyed as soon as possible and not disseminated further. As the law is written, the minimization requirements already have plenty of loopholes, including exemptions for "significant foreign intelligence information" or any "evidence of a crime." But when it comes to disseminating data to Israeli intelligence, the NSA has apparently dispensed with such legalities altogether.

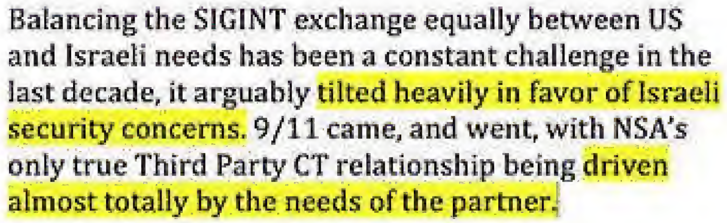
The memo flatly states: "NSA routinely sends ISNU [the Israeli SIGINT National Unit] minimized and unminimized raw collection."

Highlighting how a country can both cooperate on surveillance and be a target at the same time, an NSA document recounting the history of Israel's cooperation noted "trust issues which revolve around previous ISR operations," and identified Israel as one of the most aggressive surveillance services acting against the United States:



(TS//SI//REL) There are also a few surprises... France targets the US DoD through technical intelligence collection, and Israel also targets us. On the one hand, the Israelis are extraordinarily good SIGINT partners for us, but on the other, they target us to learn our positions on Middle East problems. A NIE [National Intelligence Estimate] ranked them as the third most aggressive intelligence service against the US.

The same report observed that, despite the close relationship between American and Israeli intelligence agencies, the extensive information provided to Israel by the United States produced little in return. Israeli intelligence was only interested in collecting data that helped them. As the NSA complained, the partnership was geared "almost totally" to Israel's needs.



Balancing the SIGINT exchange equally between US and Israeli needs has been a constant challenge in the last decade, it arguably tilted heavily in favor of Israeli security concerns. 9/11 came, and went, with NSA's only true Third Party CT relationship being driven almost totally by the needs of the partner.

Another rung lower, below the Five Eyes partners and second-tier countries such as Israel, the third tier is composed of countries who are often targets but never partners of US spying programs. Those predictably include governments viewed as adversaries, such as China, Russia, Iran, Venezuela, and Syria. But the third tier also includes countries ranging from the generally friendly to neutral, such as Brazil, Mexico, Argentina, Indonesia, Kenya, and South Africa.

* * *

When the NSA revelations first came out, the US government tried to defend its actions by saying that, unlike foreign nationals, American citizens are protected from warrantless NSA surveillance. On June 18, 2013, President Obama told

Charlie Rose: "What I can say unequivocally is that if you are a U.S. person, the NSA cannot listen to your telephone calls ... by law and by rule, and unless they ... go to a court, and obtain a warrant, and seek probable cause, the same way it's always been." The GOP chairman of the House Intelligence Committee, Mike Rogers, similarly told CNN that the NSA "is not listening to Americans' phone calls. If it did, it is illegal. It is breaking the law."

This was a rather odd line of defense: in effect, it told the rest of the world that the NSA does assault the privacy of non-Americans. Privacy protections, apparently, are only for American citizens. This message prompted such international outrage that even Facebook CEO Mark Zuckerberg, not exactly known for his vehement defense of privacy, complained that the US government "blew it" in its response to the NSA scandal by jeopardizing the interests of international Internet companies: "The government said don't worry, we're not spying on any Americans. Wonderful, that's really helpful for companies trying to work with people around the world. Thanks for going out there and being clear. I think that was really bad."

Aside from being a strange strategy, the claim is also patently false. In fact, contrary to the repeated denials of President Obama and his top officials, the NSA continuously intercepts the communications of American citizens, without any individual "probable cause" warrants to justify such surveillance. That's because the 2008 FISA law, as noted earlier, allows the NSA—without an individual warrant—to monitor the content of any American's communications as long as those communications are exchanged with a targeted foreign national. The NSA labels this "incidental" collection, as though it's some sort of minor accident that the agency has been spying on Americans. But the implication is deceitful. As Jameel Jaffer, the deputy legal director of the ACLU, explained:

> The government often says that this surveillance of Americans' communications is "incidental," which makes it sound like the NSA's surveillance of Americans' phone calls and emails is inadvertent and, even from the government's perspective, regrettable.
>
> But when the Bush administration officials asked Congress for this new surveillance power, they said quite explicitly that Americans' communications were the communications of most interest to them. See, for example, FISA for the 21st century, Hearing Before the S. Comm. On the Judiciary, 109th Cong. (2006) (statement of Michael Hayden), that certain communications "with one end in the United States" are the ones "that are most important to us."
>
> The principal purpose of the 2008 law was to make it possible for the government to collect *Americans'* international communications—and to collect those communications without reference to whether any party to those communications was doing anything illegal. And a lot of the government's advocacy is meant to obscure this fact, but it's a crucial one: The government doesn't need to "target" Americans in order to collect huge volumes of their communications.

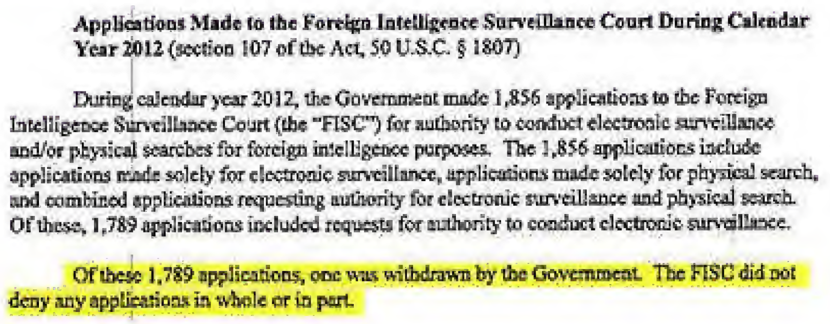
Yale Law School professor Jack Balkin concurred that the FISA law of 2008 effectively gave the president the authority to run a program "similar in effect to the warrantless surveillance program" that had been secretly implemented by George Bush. "These programs may inevitably include many phone calls involving Americans, who may have absolutely no connection to terrorism or to Al Qaeda."

Further discrediting Obama's assurances is the subservient posture of the FISA court, which grants almost every surveillance request that the NSA submits. Defenders of the NSA frequently tout the FISA court process as evidence that the agency is under effective oversight. However, the court was set up not as a genuine check on the government's power but as a cosmetic measure, providing just the appearance of reform to placate public anger over surveillance abuses revealed in the 1970s.

The uselessness of this institution as a true check on surveillance abuses is obvious because the FISA court lacks virtually every attribute of what our society generally understands as the minimal elements of a justice system. It meets in complete secrecy; only one party—the government—is permitted to attend the hearings and make its case; and the court's rulings are automatically designated "Top Secret." Tellingly, for years the FISA court was housed in the Department of Justice, making clear its role as a part of the executive branch rather than as an independent judiciary exercising real oversight.

The results have been exactly what one would expect: the court almost never rejects specific NSA applications to target Americans with surveillance. From its inception, FISA has been the ultimate rubber stamp. In its first twenty-four years, from 1978 to 2002, the court rejected a total of *zero* government applications while approving many thousands. In the subsequent decade, through 2012, the court has rejected just eleven government applications. In total, it has approved more than twenty thousand requests.

One of the provisions of the 2008 FISA law requires the executive branch annually to disclose to Congress the number of eavesdropping applications the court receives and then approves, modifies, or rejects. The disclosure for 2012 showed that the court approved every single one of the 1,788 applications for electronic surveillance that it considered, while "modifying"—that is, narrowing the purview of the order—in just 40 cases, or less than 3 percent.



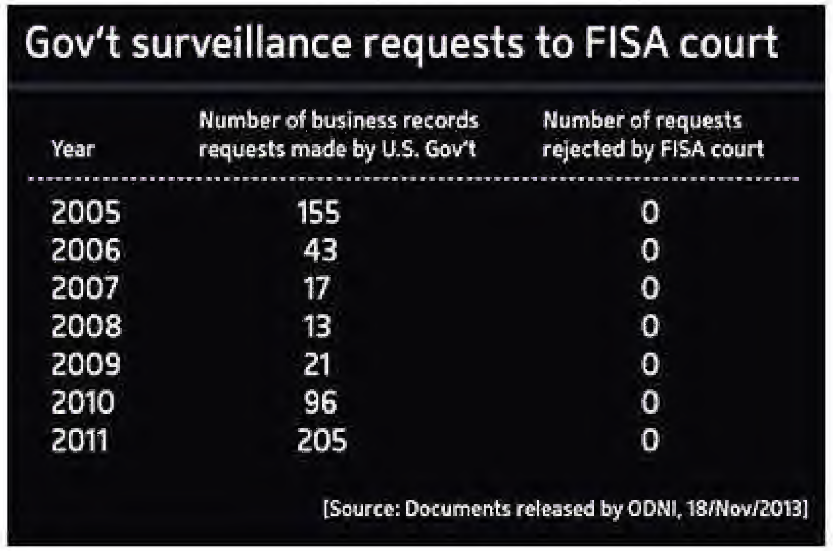
Applications Made to the Foreign Intelligence Surveillance Court During Calendar Year 2012 (section 107 of the Act, 50 U.S.C. § 1807)

During calendar year 2012, the Government made 1,856 applications to the Foreign Intelligence Surveillance Court (the "FISC") for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes. The 1,856 applications include applications made solely for electronic surveillance, applications made solely for physical search, and combined applications requesting authority for electronic surveillance and physical search. Of these, 1,789 applications included requests for authority to conduct electronic surveillance.

Of these 1,789 applications, one was withdrawn by the Government. The FISC did not deny any applications in whole or in part.

Much the same was true of 2011, when the NSA reported 1,676 applications; the FISA court, while modifying 30 of them, "did not deny any applications in whole, or in part."

The court's subservience to the NSA is demonstrated by other statistics as well. Here, for instance, is the FISA court's reaction over the last six years to various requests made by the NSA under the Patriot Act to obtain the business records—telephone, financial or medical—of US persons:



Gov't surveillance requests to FISA court

Year	Number of business records requests made by U.S. Gov't	Number of requests rejected by FISA court
2005	155	0
2006	43	0
2007	17	0
2008	13	0
2009	21	0
2010	96	0
2011	205	0

[Source: Documents released by ODNI, 18/Nov/2013]

Thus, even in those limited cases when approval from the FISA court is needed to target someone's communications, the process is more of an empty pantomime than a meaningful check on the NSA.

Another layer of oversight for the NSA is ostensibly provided by the congressional intelligence committees, also created in the aftermath of the surveillance scandals of the 1970s, but they are even more supine than the FISA court. While they are supposed to conduct "vigilant legislative oversight" over the intelligence community, those committees are in fact currently headed by the most devoted NSA loyalists in Washington: Democrat Dianne Feinstein in the Senate and Republican Mike Rogers in the House. Rather than offer any sort of adversarial check on the NSA's operations, the Feinstein and Rogers committees exist primarily to defend and justify anything the agency does.

As the *New Yorker*'s Ryan Lizza put it in a December 2013 article, instead of providing oversight, the Senate committee more often "treats senior intelligence officials like matinée idols." Observers of the committee's hearings on NSA activities were shocked by how the senators approached the questioning of NSA officials who appeared before them. The "questions" typically contained nothing more than long monologues by the senators about their recollections of the 9/11 attack and how vital it was to prevent attacks in the future. The committee members waved away the opportunity to interrogate those officials and perform their oversight responsibilities, instead propagandizing in defense of the NSA. The scene perfectly captured the true function of the intelligence committees over the last decade.

Indeed, the chairs of the congressional committees have sometimes defended the NSA even more vigorously than the agency's officials themselves have done. At one point, in August 2013, two members of Congress—Democrat Alan Grayson of Florida and Republican Morgan Griffith of Virginia—separately approached me to complain that the House Permanent Select Committee on Intelligence was blocking them and other members from accessing the most basic information about the NSA. They each gave me letters they had written to the staff of Chairman Rogers requesting information about NSA programs being discussed in the media. Those requests were rebuffed again and again.

In the wake of our Snowden stories, a group of senators from both parties who had long been concerned with surveillance abuses began efforts to draft legislation that would impose real limits on the NSA's powers. But these reformers, led by Democratic senator Ron Wyden of Oregon, ran into an immediate roadblock: counterefforts by the NSA's defenders in the Senate to write legislation that would provide only the appearance of reform, while in fact retaining or even increasing the NSA's powers. As *Slate*'s Dave Weigel reported in November:

> Critics of the NSA's bulk data collection and surveillance programs have never been worried about congressional *inaction*. They've expected Congress to come up with something that looked like reform but actually codified and excused the practices being exposed and pilloried. That's what's always happened—every amendment or reauthorization to the 2001 USA Patriot Act has built more back doors than walls.
>
> "We will be up against a 'business-as-usual brigade'—made up of influential members of the government's intelligence leadership, their allies in thinktanks [*sic*] and academia, retired government officials, and sympathetic legislators," warned Oregon Sen. Ron Wyden last month. "Their endgame is ensuring that any surveillance reforms are only skin-deep.... Privacy protections that don't actually protect privacy are not worth the paper they're printed on."

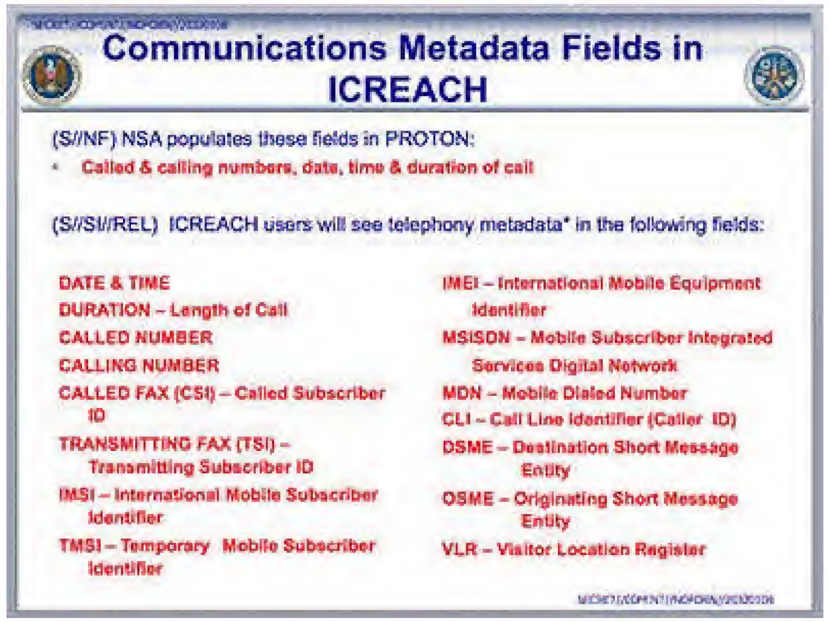
The "fake reform" faction was led by Dianne Feinstein, the very senator who is charged with exercising primary oversight over the NSA. Feinstein has long been a devoted loyalist of the US national security industry, from her vehement support for the war on Iraq to her steadfast backing of Bush-era NSA programs. (Her husband, meanwhile, has major stakes in various military contracts.) Clearly, Feinstein was a natural choice to head a committee that claims to carry out oversight over the intelligence community but has for years performed the opposite function.

Thus, for all the government's denials, the NSA has no substantial constraints on whom it can spy on and how. Even when such constraints nominally exist—when American citizens are the surveillance target—the process has become largely hollow. The NSA is the definitive rogue agency: empowered to do whatever it wants with very little control, transparency, or accountability.

* * *

Very broadly speaking, the NSA collects two types of information: content and metadata. "Content" here refers to actually listening to people's phone calls or reading their emails and online chats, as well as reviewing Internet activity such as browsing histories and search activities. "Metadata" collection, meanwhile, involves amassing data *about* those communications. The NSA refers to that as "information about content (but not the content itself)."

Metadata about an email message, for instance, records who emailed whom, when the email was sent, and the location of the person sending it. When it comes to telephone calls, the information includes the phone numbers of the caller and the receiver, how long they spoke for, and often their locations and the types of devices they used to communicate. In one document about telephone calls, the NSA outlined the metadata it accesses and stores:



Communications Metadata Fields in ICREACH

(S//NF) NSA populates these fields in PROTON:

- Called & calling numbers, date, time & duration of call

(S//SI//REL) ICREACH users will see telephony metadata* in the following fields:

DATE & TIME
DURATION – Length of Call
CALLED NUMBER
CALLING NUMBER
CALLED FAX (CSI) – Called Subscriber ID
TRANSMITTING FAX (TSI) – Transmitting Subscriber ID
IMSI – International Mobile Subscriber Identifier
TMSI – Temporary Mobile Subscriber Identifier
IMEI – International Mobile Equipment Identifier
MSISDN – Mobile Subscriber Integrated Services Digital Network
MDN – Mobile Dialed Number
CLI – Call Line Identifier (Caller ID)
DSME – Destination Short Message Entity
OSME – Originating Short Message Entity
VLR – Visitor Location Register

The US government has insisted that much of the surveillance revealed in the Snowden archive involves the collection of "metadata, not content," trying to imply that this kind of spying is not intrusive—or at least not to the same degree as intercepting content. Dianne Feinstein has explicitly argued in *USA Today* that the metadata collection of all Americans' telephone records "is not surveillance" at all because it "does not collect the content of any communication."

These disingenuous arguments obscure the fact that metadata surveillance can be at least as intrusive as content interception, and often even more so. When the government knows everyone you call and everyone who calls you, plus the exact length of all those phone conversations; when it can list every single one of your email correspondents and every location from where your emails were sent, it can create a remarkably comprehensive picture of your life, your associations, and your activities, including some of your most intimate and private information.

In an affidavit filed by the ACLU challenging the legality of the NSA's metadata collection program, Princeton computer science and public affairs professor Edward Felten explained why metadata surveillance can be especially revealing:

> Consider the following hypothetical example: A young woman calls her gynecologist; then immediately calls her mother; then a man who, during the past few months, she had repeatedly spoken to on the telephone after 11pm; followed by a call to a family planning center that also offers abortions. A likely storyline emerges that would not be as evident by examining the record of a single telephone call.

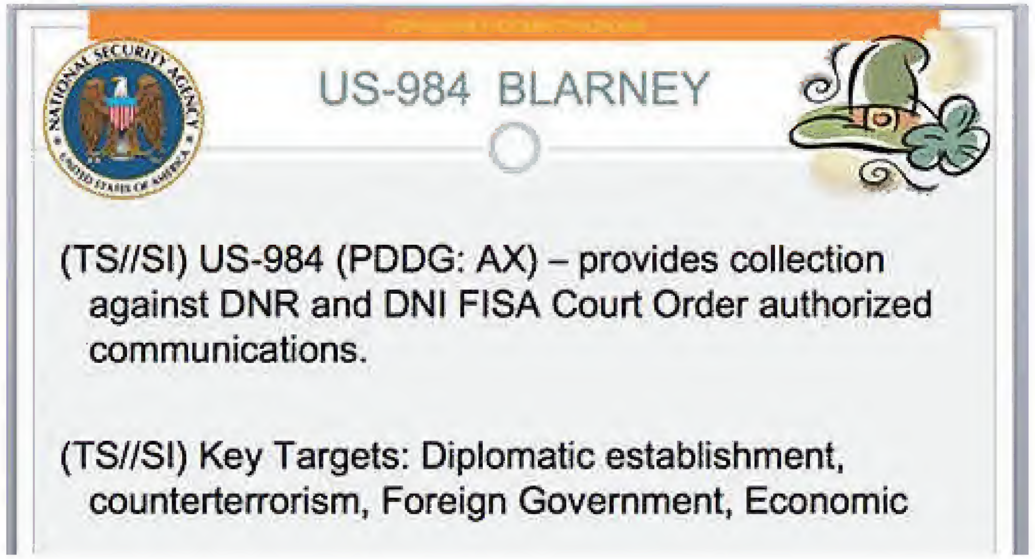
Even for a single phone call, the metadata can be more informative than the call's content. Listening in on a woman calling an abortion clinic might reveal nothing more than someone confirming an appointment with a generic-sounding establishment ("East Side Clinic" or "Dr. Jones's office"). But the metadata would show far more than that: it would reveal the identity of those who were called. The same is true of calls to a dating service, a gay and lesbian center, a drug addiction clinic, an HIV specialist, or a suicide hotline. Metadata would likewise unmask a conversation between a human rights activist and an informant in a repressive regime, or a confidential source calling a journalist to reveal high-level wrongdoing. And if you frequently call someone late at night who is not your spouse, the metadata will reveal that, too. What's more, it will record not only all the people with whom you communicate and how often, but also all the people with whom your friends and associates communicate, creating a comprehensive picture of your network of contacts.

Indeed, as Professor Felten notes, eavesdropping on calls can be quite difficult due to language differences, meandering conversations, the use of slang or deliberate codes, and other attributes that either by design or accident obfuscate the meaning. "The content of calls are far more difficult to analyze in an automated fashion due to their unstructured nature," he argued. By contrast, metadata is mathematical: clean, precise, and thus easily analyzed. And as Felten put it, it is often "a proxy for content":

> Telephony metadata can ... expose an extraordinary amount about our habits and our associations. Calling patterns can reveal when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath, or makes a large number of calls on Christmas day; our work habits and our social aptitude; the number of friends we have; and even our civil and political affiliations.

In sum, writes Felten, "mass collection not only allows the government to learn information about more people, but it also enables the government to learn new, previously private facts that it could not have learned simply by collecting the information about a few, specific individuals."

Concern about the many uses that the government could find for this kind of sensitive information is especially justified because, contrary to repeated claims from President Obama and the NSA, it is already clear that a substantial number of the agency's activities have nothing to do with antiterrorism efforts or even with national security. Much of the Snowden archive revealed what can only be called economic espionage: eavesdropping and email interception aimed at the Brazilian oil giant Petrobras, economic conferences in Latin America, energy companies in Venezuela

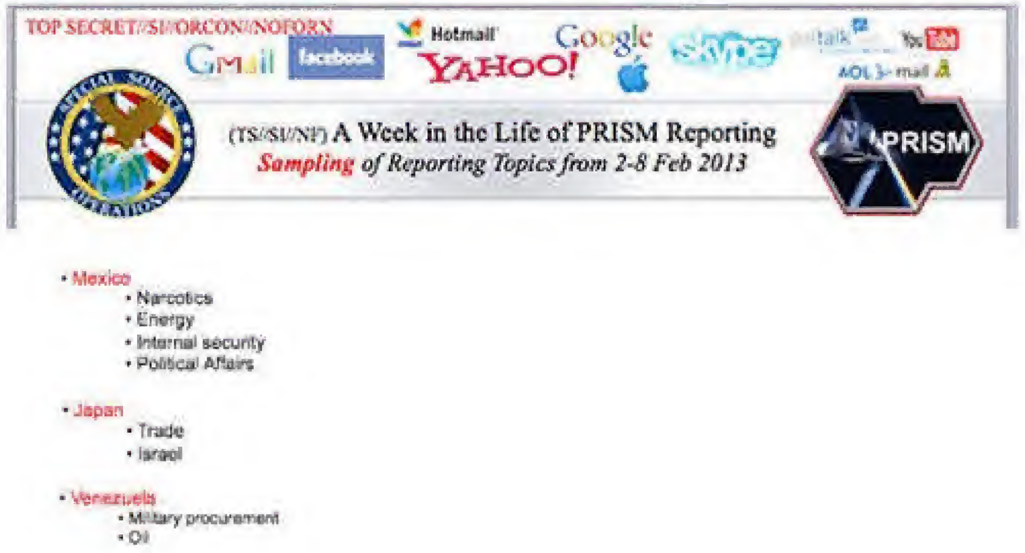


US-984 BLARNEY

(TS//SI) US-984 (PDDG: AX) – provides collection against DNR and DNI FISA Court Order authorized communications.

(TS//SI) Key Targets: Diplomatic establishment, counterterrorism, Foreign Government, Economic

Further evidence of the NSA's economic interest appears in a PRISM document showing a "sampling" of the "Reporting Topics" for the week of February 2–8, 2013. A list of the types of information gathered from various countries clearly includes economic and financial categories, among them "energy," "trade," and "oil":



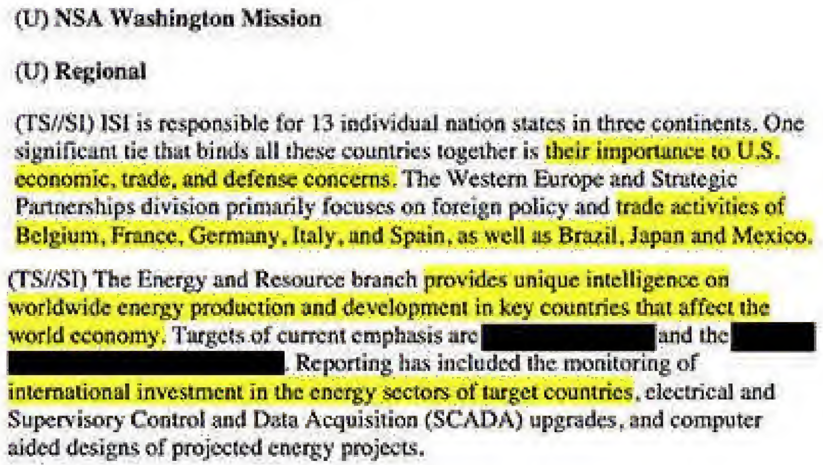
TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) A Week in the Life of PRISM Reporting

Sampling of Reporting Topics from 2-8 Feb 2013

- Mexico
  - Narcotics
  - Energy
  - Internal security
  - Political Affairs
- Japan
  - Trade
  - Israel
- Venezuela
  - Military procurement
  - Oil

One 2006 memorandum from the global capabilities manager of the agency's International Security Issues (ISI) mission spells out the NSA's economic and trade espionage—against countries as diverse as Belgium, Japan, Brazil, and Germany—in stark terms:



(U) NSA Washington Mission

(U) Regional

(TS//SI) ISI is responsible for 13 individual nation states in three continents. One significant tie that binds all these countries together is their importance to U.S. economic, trade, and defense concerns. The Western Europe and Strategic Partnerships division primarily focuses on foreign policy and trade activities of Belgium, France, Germany, Italy, and Spain, as well as Brazil, Japan and Mexico.

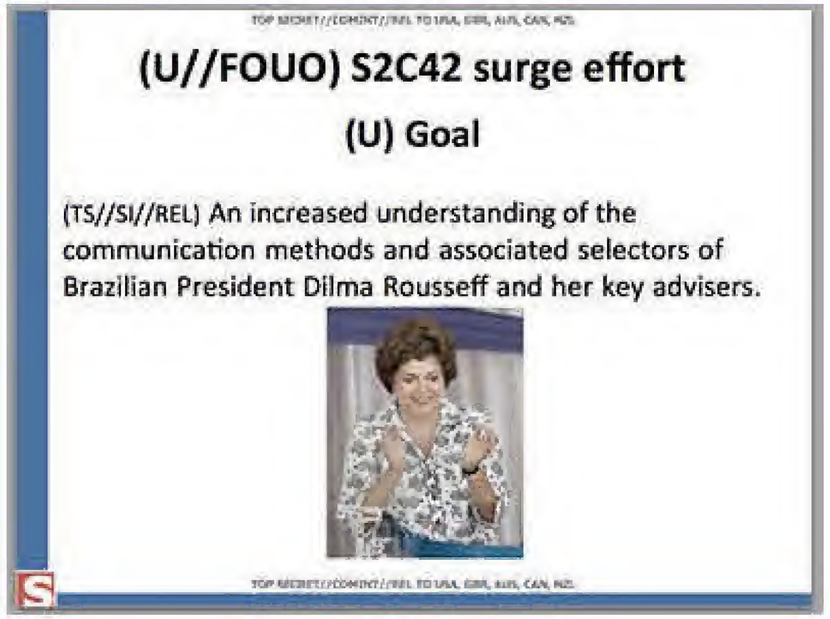
(TS//SI) The Energy and Resource branch provides unique intelligence on worldwide energy production and development in key countries that affect the world economy. Targets of current emphasis are [redacted] and the [redacted]. Reporting has included the monitoring of international investment in the energy sectors of target countries, electrical and Supervisory Control and Data Acquisition (SCADA) upgrades, and computer aided designs of projected energy projects.

Reporting on a group of GCHQ documents leaked by Snowden, the *New York Times* noted that its surveillance targets often included financial institutions and "heads of international aid organizations, foreign energy companies and a European Union official involved in antitrust battles with American technology businesses." It added that the US and British agencies "monitored the communications of senior European Union officials, foreign leaders including African heads of state and sometimes their family members, directors of United Nations and other relief programs [such as UNICEF], and officials overseeing oil and finance ministries."

The reasons for economic espionage are clear enough. When the United States uses the NSA to eavesdrop on the planning strategies of other countries during trade and economic talks, it can gain enormous advantage for American industry. In 2009, for example, Assistant Secretary of State Thomas Shannon wrote a letter to Keith Alexander, offering his "gratitude and congratulations for the outstanding signals intelligence support" that the State Department received regarding the Fifth Summit of the Americas, a conference devoted to negotiating economic accords. In the letter, Shannon specifically noted that the NSA's surveillance provided the United States with negotiating advantages over the other parties:

> The more than 100 reports we received from the NSA gave us deep insight into the plans and intentions of other Summit participants, and ensured that our diplomats were well prepared to advise President Obama and Secretary Clinton on how to deal with contentious issues, such as Cuba, and interact with difficult counterparts, such as Venezuelan President Chavez.

The NSA is equally devoted to diplomatic espionage, as the documents referring to "political affairs" demonstrate. One particularly egregious example, from 2011, shows how the agency targeted two Latin American leaders—Dilma Rousseff, the president of Brazil, along with "her key advisers"; and Enrique Peña Nieto, then Mexico's leading presidential candidate (and now its president), along with "nine of his close associates"—for a "surge" of especially invasive surveillance. The document even features some of the intercepted text messages sent and received by Nieto and a "close associate":



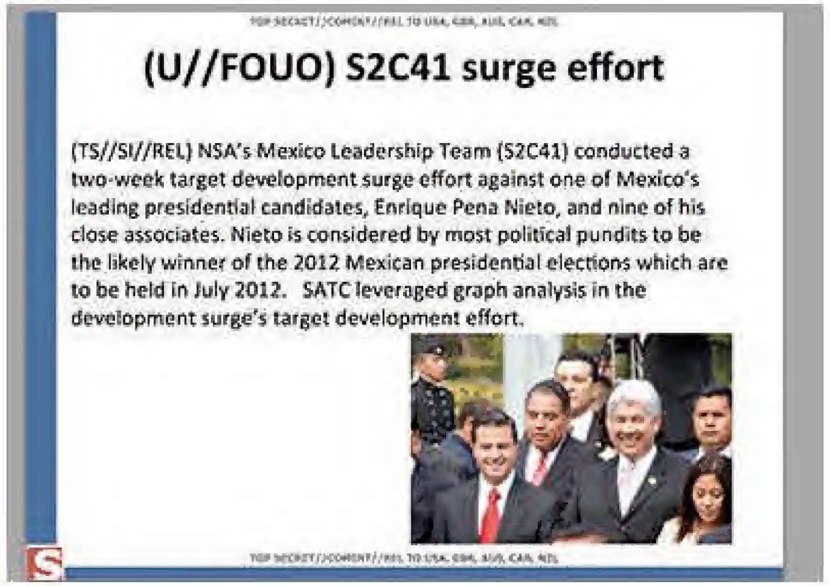
TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U//FOUO) S2C42 surge effort

(U) Goal

(TS//SI//REL) An increased understanding of the communication methods and associated selectors of Brazilian President Dilma Rousseff and her key advisers.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL



TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U//FOUO) S2C41 surge effort

(TS//SI//REL) NSA's Mexico Leadership Team (S2C41) conducted a two-week target development surge effort against one of Mexico's leading presidential candidates, Enrique Pena Nieto, and nine of his close associates. Nieto is considered by most political pundits to be the likely winner of the 2012 Mexican presidential elections which are to be held in July 2012. SATC leveraged graph analysis in the development surge's target development effort.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U) Results

- (S//SI//REL)85489 Text messages

Interesting Messages

[redacted] [illegible] Jorge Corona [illegible] [redacted]

- (TS//SI//REL) Number for Travel coordinator
- (TS//SI//REL) Jorge Corona – Close associate of Nieto

[redacted] .Mi Querido Alex el nuevo titular de Com. Social es Juan Ramon Flores su cel es [redacted] el [redacted] Nuevo Srio. Part. [illegible] [redacted] el Nuevo [illegible] JORGE CORONA es [redacted] [illegible] y seguimos en contacto avisame el llego el [illegible] por favor...... [redacted]

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U) Conclusion

- (S//REL) Contact graph-enhanced filtering is a simple yet effective technique, which may allow you to find previously unobtainable results and empower analytic discovery
- (TS//SI//REL) Teaming with S2C, SATC was able to successfully apply this technique against high-profile, OPSEC-savvy Brazilian and Mexican targets.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

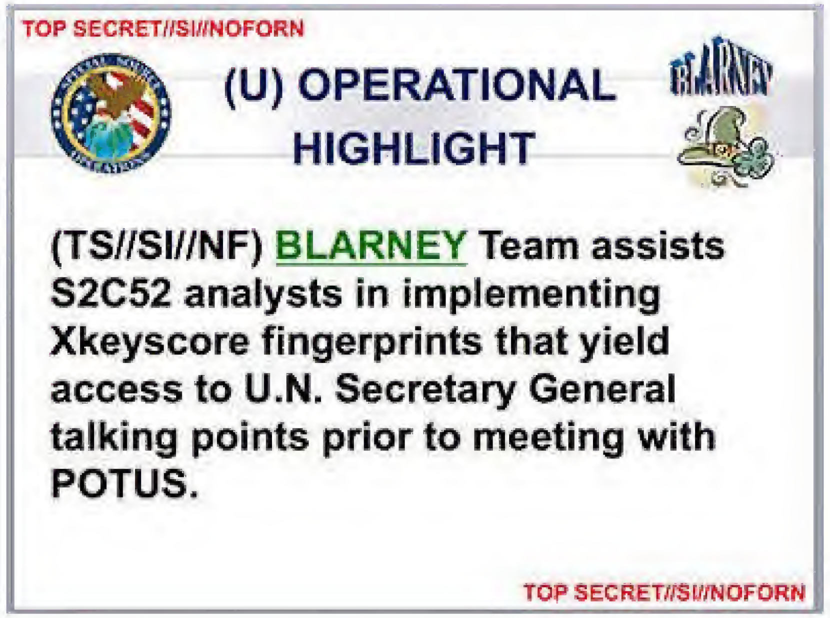
One can speculate about why political leaders of Brazil and Mexico were NSA targets. Both countries are rich in oil resources. They are a big and influential presence in the region. And while they are far from adversaries, they are also not America's closest and most trusted allies. Indeed, one NSA planning document—entitled "Identifying Challenges: Geopolitical Trends for 2014–2019"—list both Mexico and Brazil under the heading "Friends, Enemies, or Problems?" Others on that list are Egypt, India, Iran, Saudi Arabia, Somalia, Sudan, Turkey, and Yemen.

But ultimately, in this case as in most others, speculation about any specific target is based on a false premise. The NSA does not need any specific reason or rationale to invade people's private communications. Their institutional mission is to collect everything.

If anything, the revelations about NSA spying on foreign leaders are *less* significant than the agency's warrantless mass surveillance of whole populations. Countries have spied on heads of state for centuries, including allies. This is unremarkable, despite the great outcry that ensued when, for example, the world discovered that the NSA had for many years targeted the personal cell phone of German chancellor Angela Merkel.

More remarkable is the fact that in country after country, revelations that the NSA was spying on hundreds of millions of their citizens produced little more than muted objections from their political leadership. True indignation came gushing forward only once those leaders understood that they, and not just their citizens, had been targeted as well.

Still, the sheer scale of diplomatic surveillance the NSA has practiced is unusual and noteworthy. In addition to foreign leaders, the United States has also, for example, spied extensively on international organizations such as the United Nations to gain diplomatic advantage. One April 2013 briefing from SSO is typical, noting how the agency used its programs to obtain the UN secretary general's talking points prior to his meeting with President Obama:



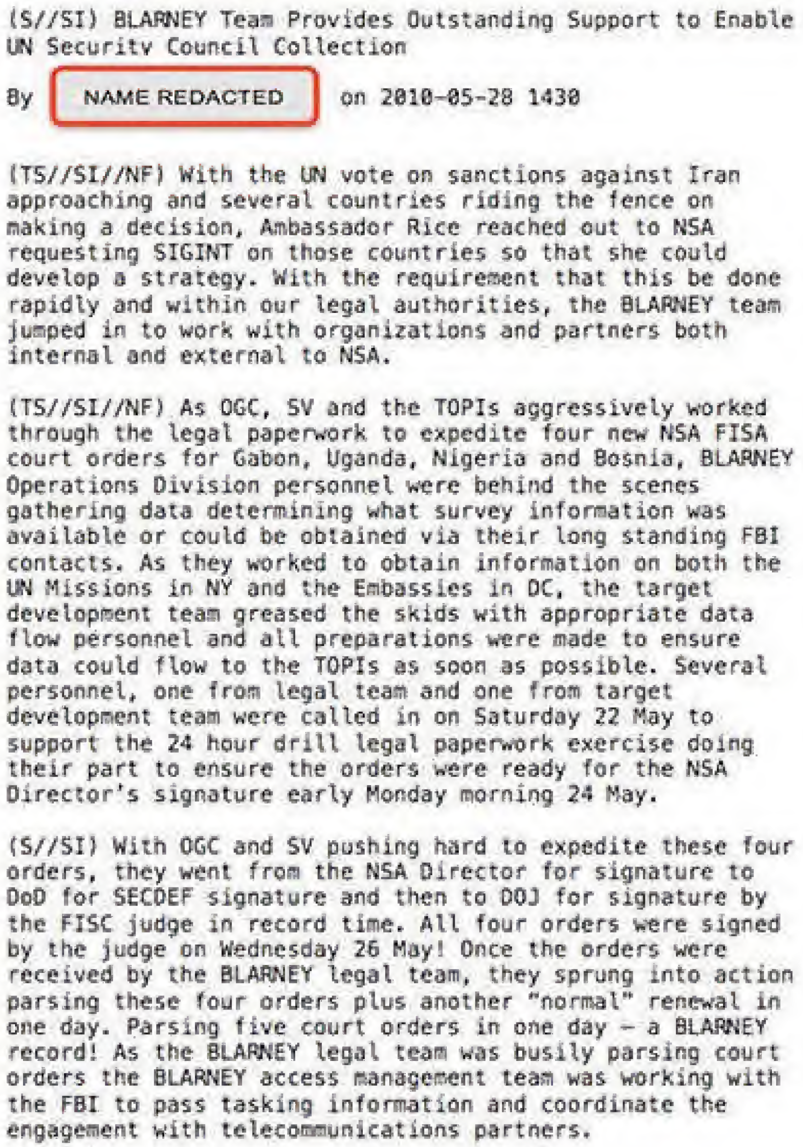
TOP SECRET//SI//NOFORN

(U) OPERATIONAL HIGHLIGHT

(TS//SI//NF) BLARNEY Team assists S2C52 analysts in implementing Xkeyscore fingerprints that yield access to U.N. Secretary General talking points prior to meeting with POTUS.

TOP SECRET//SI//NOFORN

Numerous other documents detail how Susan Rice, then ambassador to the UN and now President Obama's national security adviser, repeatedly requested that the NSA spy on the internal discussions of key member states to learn their negotiation strategies. A May 2010 SSO report describes this process in connection with a resolution being debated by the UN that involved imposing new sanctions on Iran.



(S//SI) BLARNEY Team Provides Outstanding Support to Enable UN Security Council Collection

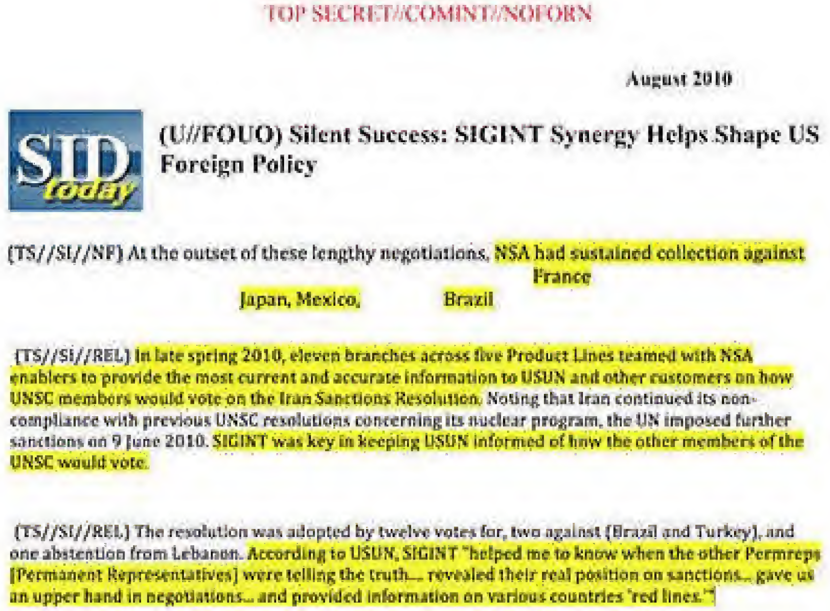
By NAME REDACTED on 2010-05-28 1430

(TS//SI//NF) With the UN vote on sanctions against Iran approaching and several countries riding the fence on making a decision, Ambassador Rice reached out to NSA requesting SIGINT on those countries so that she could develop a strategy. With the requirement that this be done rapidly and within our legal authorities, the BLARNEY team jumped in to work with organizations and partners both internal and external to NSA.

(TS//SI//NF) As OGC, SV and the TOPIs aggressively worked through the legal paperwork to expedite four new NSA FISA court orders for Gabon, Uganda, Nigeria and Bosnia, BLARNEY Operations Division personnel were behind the scenes gathering data determining what survey information was available or could be obtained via their long standing FBI contacts. As they worked to obtain information on both the UN Missions in NY and the Embassies in DC, the target development team greased the skids with appropriate data flow personnel and all preparations were made to ensure data could flow to the TOPIs as soon as possible. Several personnel, one from legal team and one from target development team were called in on Saturday 22 May to support the 24 hour drill legal paperwork exercise doing their part to ensure the orders were ready for the NSA Director's signature early Monday morning 24 May.

(S//SI) With OGC and SV pushing hard to expedite these four orders, they went from the NSA Director for signature to DoD for SECDEF signature and then to DOJ for signature by the FISC judge in record time. All four orders were signed by the judge on Wednesday 26 May! Once the orders were received by the BLARNEY legal team, they sprung into action parsing these four orders plus another "normal" renewal in one day. Parsing five court orders in one day – a BLARNEY record! As the BLARNEY legal team was busily parsing court orders the BLARNEY access management team was working with the FBI to pass tasking information and coordinate the engagement with telecommunications partners.

A similar surveillance document from August 2010 reveals that the United States spied on eight members of the UN Security Council regarding a subsequent resolution about sanctions on Iran. The list included France, Brazil, Japan, and Mexico—all considered friendly nations. The espionage gave the US government valuable information about those countries' voting intentions, giving Washington an edge when talking to other members of the Security Council.



TOP SECRET//COMINT//NOFORN

August 2010

SID today

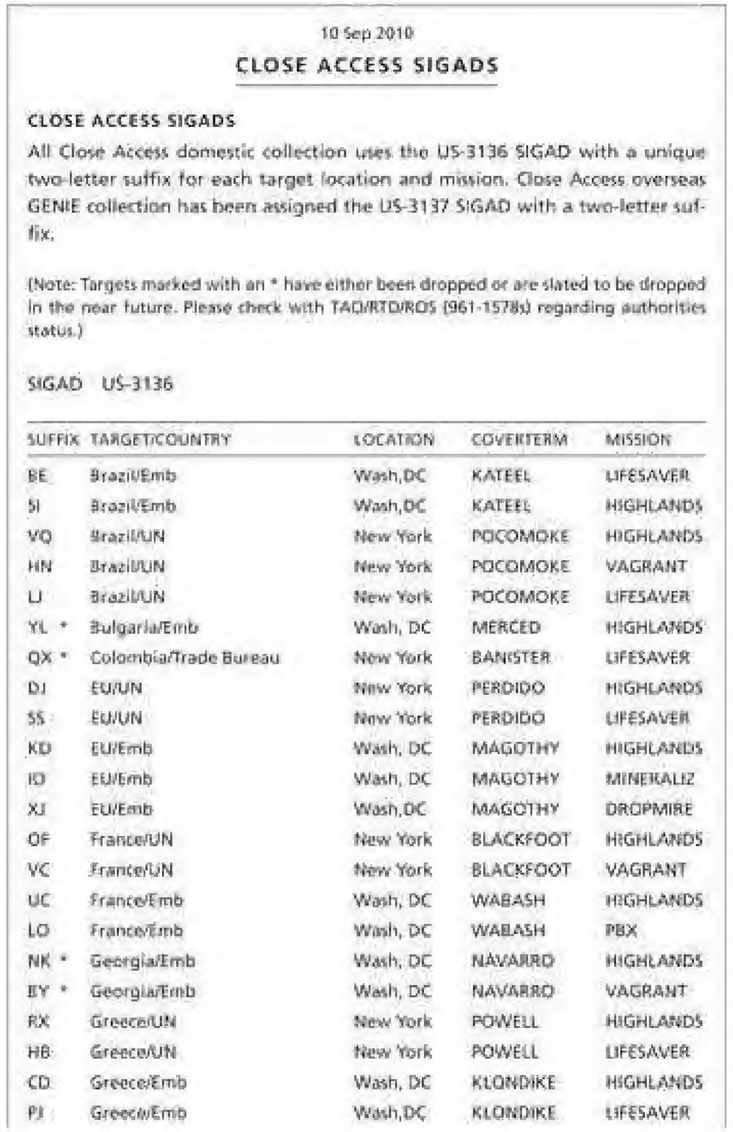
(U//FOUO) Silent Success: SIGINT Synergy Helps Shape US Foreign Policy

(TS//SI//NF) At the outset of these lengthy negotiations, NSA had sustained collection against France Japan, Mexico, Brazil

(TS//SI//REL) In late spring 2010, eleven branches across five Product Lines teamed with NSA enablers to provide the most current and accurate information to USUN and other customers on how UNSC members would vote on the Iran Sanctions Resolution. Noting that Iran continued its non-compliance with previous UNSC resolutions concerning its nuclear program, the UN imposed further sanctions on 9 June 2010. SIGINT was key in keeping USUN informed of how the other members of the UNSC would vote.

(TS//SI//REL) The resolution was adopted by twelve votes for, two against (Brazil and Turkey), and one abstention from Lebanon. According to USUN, SIGINT "helped me to know when the other Permreps [Permanent Representatives] were telling the truth... revealed their real position on sanctions... gave us an upper hand in negotiations... and provided information on various countries 'red lines.'"

To facilitate diplomatic spying, the NSA has gained various forms of access to the embassies and consulates of many of its closest allies. One 2010 document—shown here with some countries deleted—lists the nations whose diplomatic structures inside the United States were invaded by the agency. A glossary at the end explains the various types of surveillance used.



10 Sep 2010

CLOSE ACCESS SIGADS

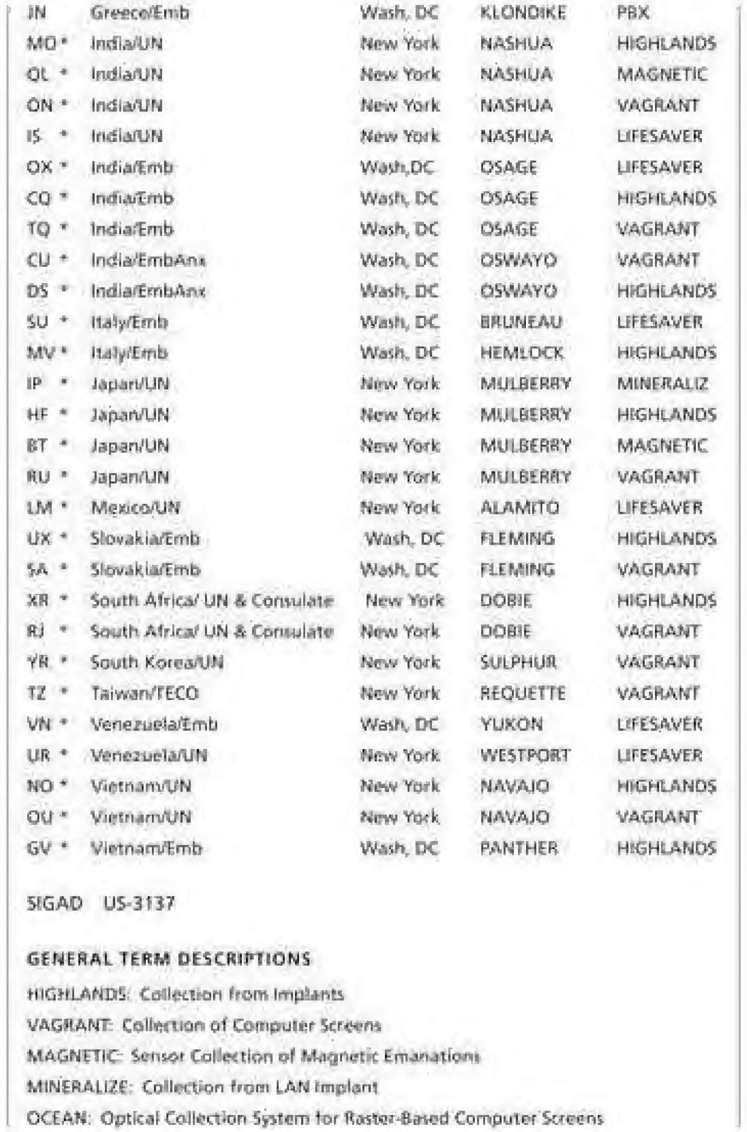
CLOSE ACCESS SIGADS

All Close Access domestic collection uses the US-3136 SIGAD with a unique two-letter suffix for each target location and mission. Close Access overseas GENIE collection has been assigned the US-3137 SIGAD with a two-letter suffix.

(Note: Targets marked with an * have either been dropped or are slated to be dropped in the near future. Please check with TAO/RTD/ROS (961-1578s) regarding authorities status.)

SIGAD US-3136

SUFFIX	TARGET/COUNTRY	LOCATION	COVERTERM	MISSION
BE	Brazil/Emb	Wash,DC	KATEEL	LIFESAVER
SI	Brazil/Emb	Wash,DC	KATEEL	HIGHLANDS
VQ	Brazil/UN	New York	POCOMOKE	HIGHLANDS
HN	Brazil/UN	New York	POCOMOKE	VAGRANT
LJ	Brazil/UN	New York	POCOMOKE	LIFESAVER
YL *	Bulgaria/Emb	Wash, DC	MERCED	HIGHLANDS
QX *	Colombia/Trade Bureau	New York	BANISTER	LIFESAVER
DJ	EU/UN	New York	PERDIDO	HIGHLANDS
SS	EU/UN	New York	PERDIDO	LIFESAVER
KD	EU/Emb	Wash, DC	MAGOTHY	HIGHLANDS
IO	EU/Emb	Wash, DC	MAGOTHY	MINERALIZ
XJ	EU/Emb	Wash,DC	MAGOTHY	DROPMIRE
OF	France/UN	New York	BLACKFOOT	HIGHLANDS
VC	France/UN	New York	BLACKFOOT	VAGRANT
UC	France/Emb	Wash, DC	WABASH	HIGHLANDS
LO	France/Emb	Wash, DC	WABASH	PBX
NK *	Georgia/Emb	Wash, DC	NAVARRO	HIGHLANDS
BY *	Georgia/Emb	Wash, DC	NAVARRO	VAGRANT
RX	Greece/UN	New York	POWELL	HIGHLANDS
HB	Greece/UN	New York	POWELL	LIFESAVER
CD	Greece/Emb	Wash, DC	KLONDIKE	HIGHLANDS
PJ	Greece/Emb	Wash,DC	KLONDIKE	LIFESAVER
JN	Greece/Emb	Wash, DC	KLONDIKE	PBX
MO *	India/UN	New York	NASHUA	HIGHLANDS
QL *	India/UN	New York	NASHUA	MAGNETIC
ON *	India/UN	New York	NASHUA	VAGRANT
IS *	India/UN	New York	NASHUA	LIFESAVER
OX *	India/Emb	Wash,DC	OSAGE	LIFESAVER
CQ *	India/Emb	Wash, DC	OSAGE	HIGHLANDS
TQ *	India/Emb	Wash, DC	OSAGE	VAGRANT
CU *	India/EmbAnx	Wash, DC	OSWAYO	VAGRANT
DS *	India/EmbAnx	Wash, DC	OSWAYO	HIGHLANDS
SU *	Italy/Emb	Wash, DC	BRUNEAU	LIFESAVER
MV *	Italy/Emb	Wash, DC	HEMLOCK	HIGHLANDS
IP *	Japan/UN	New York	MULBERRY	MINERALIZ
HF *	Japan/UN	New York	MULBERRY	HIGHLANDS
BT *	Japan/UN	New York	MULBERRY	MAGNETIC
RU *	Japan/UN	New York	MULBERRY	VAGRANT
LM *	Mexico/UN	New York	ALAMITO	LIFESAVER
UX *	Slovakia/Emb	Wash, DC	FLEMING	HIGHLANDS
SA *	Slovakia/Emb	Wash, DC	FLEMING	VAGRANT
XR *	South Africa/ UN & Consulate	New York	DOBIE	HIGHLANDS
RJ *	South Africa/ UN & Consulate	New York	DOBIE	VAGRANT
YR *	South Korea/UN	New York	SULPHUR	VAGRANT
TZ *	Taiwan/TECO	New York	REQUETTE	VAGRANT
VN *	Venezuela/Emb	Wash, DC	YUKON	LIFESAVER
UR *	Venezuela/UN	New York	WESTPORT	LIFESAVER
NO *	Vietnam/UN	New York	NAVAJO	HIGHLANDS
OU *	Vietnam/UN	New York	NAVAJO	VAGRANT
GV *	Vietnam/Emb	Wash, DC	PANTHER	HIGHLANDS



SIGAD US-3137

GENERAL TERM DESCRIPTIONS

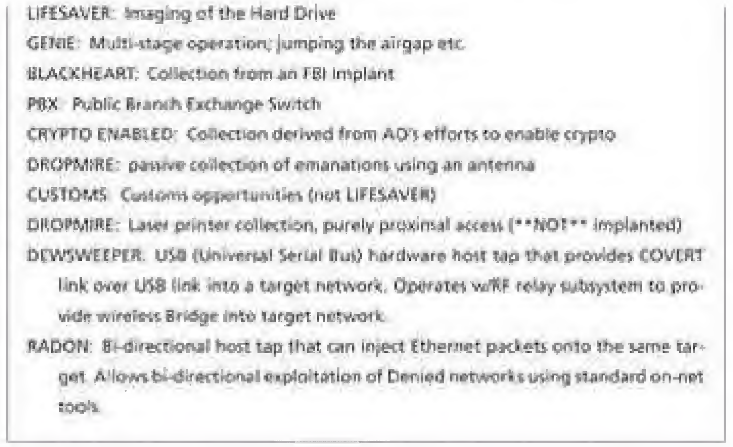
HIGHLANDS: Collection from Implants

VAGRANT: Collection of Computer Screens

MAGNETIC: Sensor Collection of Magnetic Emanations

MINERALIZE: Collection from LAN Implant

OCEAN: Optical Collection System for Raster-Based Computer Screens



LIFESAVER: Imaging of the Hard Drive

GENIE: Multi-stage operation; jumping the airgap etc.

BLACKHEART: Collection from an FBI Implant

PBX: Public Branch Exchange Switch

CRYPTO ENABLED: Collection derived from AO's efforts to enable crypto

DROPMIRE: passive collection of emanations using an antenna

CUSTOMS: Customs opportunities (not LIFESAVER)

DROPMIRE: Laser printer collection, purely proximal access (**NOT** implanted)

DEWSWEEPER: USB (Universal Serial Bus) hardware host tap that provides COVERT link over USB link into a target network. Operates w/RF relay subsystem to provide wireless Bridge into target network.

RADON: Bi-directional host tap that can inject Ethernet packets onto the same target. Allows bi-directional exploitation of Denied networks using standard on-net tools.

Some of the NSA's methods serve all agendas—economic, diplomatic, security, and obtaining an all-purpose global advantage—and these are among the most invasive, and hypocritical, in the agency's repertoire. For years, the US government loudly warned the world that Chinese routers and other Internet devices pose a "threat" because they are built with backdoor surveillance functionality that gives the Chinese government the ability to spy on anyone using them. Yet what the NSA's documents show is that Americans have been engaged in precisely the activity that the United States accused the Chinese of doing.

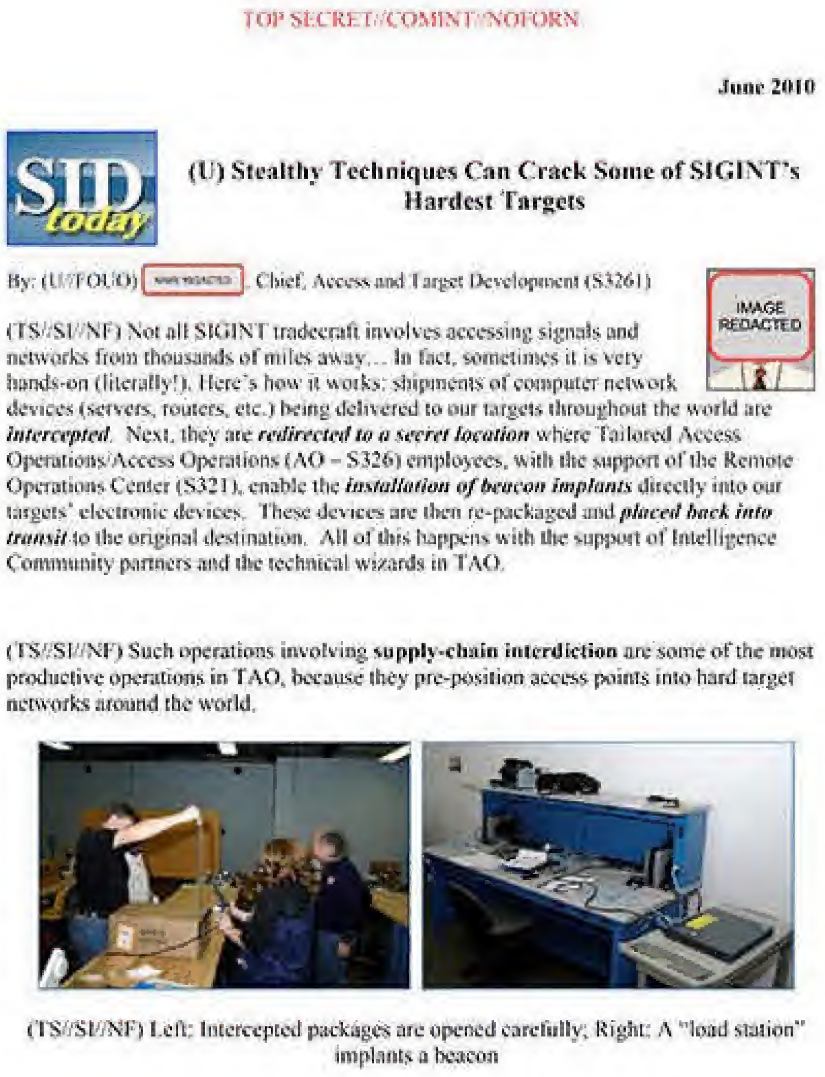
The drumbeat of American accusations against Chinese Internet device manufacturers was unrelenting. In 2012, for example, a report from the House Intelligence Committee, headed by Mike Rogers, claimed that Huawei and ZTE, the top two Chinese telecommunications equipment companies, "may be violating United States laws" and have "not followed United States legal obligations or international standards of business behavior." The committee recommended that "the United States should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies."

The Rogers committee voiced fears that the two companies were enabling Chinese state surveillance, although it acknowledged that it had obtained no actual evidence that the firms had implanted their routers and other systems with surveillance devices. Nonetheless, it cited the failure of those companies to cooperate and urged US firms to avoid purchasing their products:

> Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects. Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems.

The constant accusations became such a burden that Ren Zhengfei, the sixty-nine-year-old founder and CEO of Huawei, announced in November 2013 that the company was abandoning the US market. As *Foreign Policy* reported, Zhengfei told a French newspaper: "'If Huawei gets in the middle of U.S-China relations,' and causes problems, 'it's not worth it.'"

But while American companies were being warned away from supposedly untrustworthy Chinese routers, foreign organizations would have been well advised to beware of American-made ones. A June 2010 report from the head of the NSA's Access and Target Development department is shockingly explicit. The NSA routinely receives—or intercepts —routers, servers, and other computer network devices being exported from the United States before they are delivered to the international customers. The agency then implants backdoor surveillance tools, repackages the devices with a factory seal, and sends them on. The NSA thus gains access to entire networks and all their users. The document gleefully observes that some "SIGINT tradecraft ... is very hands-on (literally!)":



TOP SECRET//COMINT//NOFORN

June 2010

(U) Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets

By: (U//FOUO) NAME REDACTED, Chief, Access and Target Development (S3261)

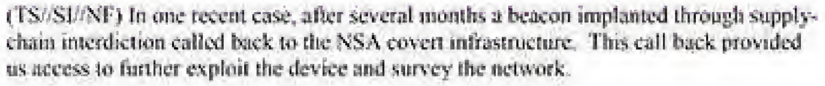
IMAGE REDACTED

(TS//SI//NF) Not all SIGINT tradecraft involves accessing signals and networks from thousands of miles away... In fact, sometimes it is very hands-on (literally!). Here's how it works: shipments of computer network devices (servers, routers, etc.) being delivered to our targets throughout the world are ***intercepted***. Next, they are ***redirected to a secret location*** where Tailored Access Operations/Access Operations (AO – S326) employees, with the support of the Remote Operations Center (S321), enable the ***installation of beacon implants*** directly into our targets' electronic devices. These devices are then re-packaged and ***placed back into transit*** to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO.

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

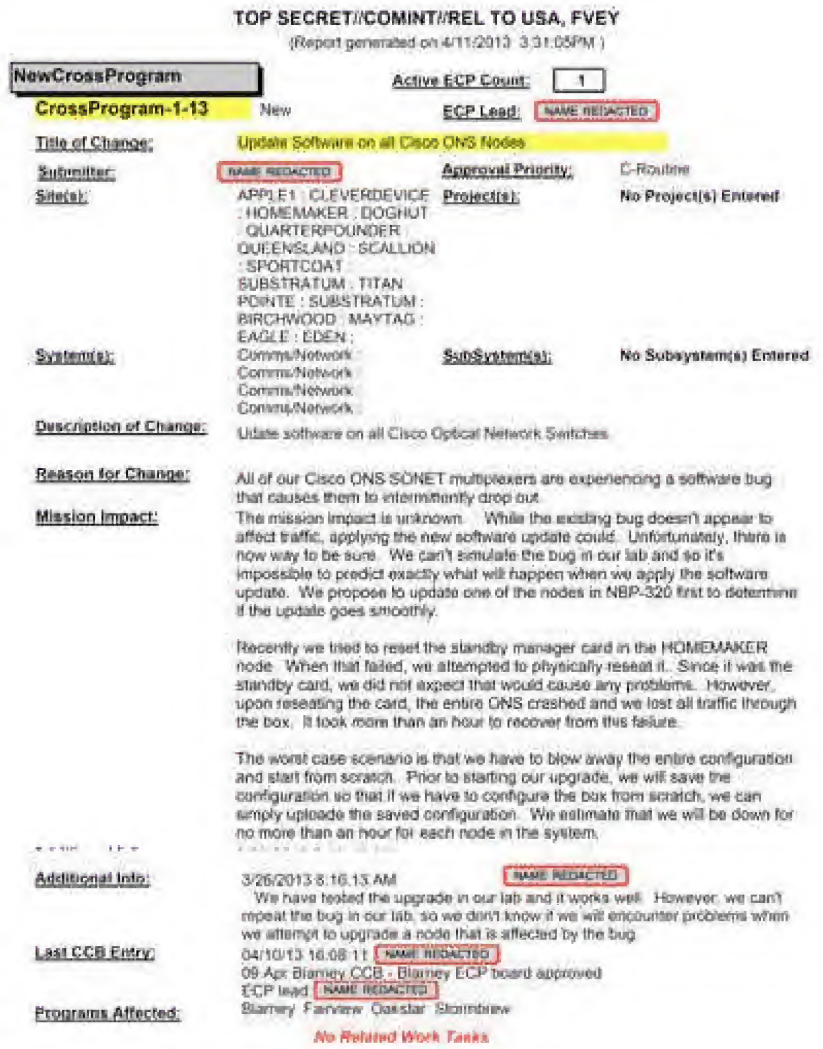
(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

Eventually, the implanted device connects back to the NSA infrastructure:



(TS//SI//NF) In one recent case, after several months a beacon implanted through supply-chain interdiction called back to the NSA covert infrastructure. This call back provided us access to further exploit the device and survey the network.

Among other devices, the agency intercepts and tampers with routers and servers manufactured by Cisco to direct large amounts of Internet traffic back to the NSA's repositories. (There is no evidence in the documents that Cisco is aware of, or condoned, these interceptions.) In April 2013, the agency grappled with technical difficulties involving the intercepted Cisco network switches, which affected the BLARNEY, FAIRVIEW, OAKSTAR, and STORMBREW programs:



TOP SECRET//COMINT//REL TO USA, FVEY

(Report generated on 4/11/2013 3:31:05PM)

NewCrossProgram

Active ECP Count: 1

CrossProgram-1-13 New

ECP Lead: NAME REDACTED

Title of Change: Update Software on all Cisco ONS Nodes

Submitter: NAME REDACTED

Approval Priority: C-Routine

Site(s): APPLE1 : CLEVERDEVICE : HOMEMAKER : DOGHUT : QUARTERPOUNDER : QUEENSLAND : SCALLION : SPORTCOAT : SUBSTRATUM : TITAN POINTE : SUBSTRATUM : BIRCHWOOD : MAYTAG : EAGLE : EDEN ;

Project(s): No Project(s) Entered

System(s): Comms/Network : Comms/Network : Comms/Network : Comms/Network :

SubSystem(s): No Subsystem(s) Entered

Description of Change: Udate software on all Cisco Optical Network Switches

Reason for Change: All of our Cisco ONS SONET multiplexers are experiencing a software bug that causes them to intermittently drop out.

Mission Impact: The mission impact is unknown. While the existing bug doesn't appear to affect traffic, applying the new software update could. Unfortunately, there is now way to be sure. We can't simulate the bug in our lab and so it's impossible to predict exactly what will happen when we apply the software update. We propose to update one of the nodes in NBP-320 first to determine if the update goes smoothly.

Recently we tried to reset the standby manager card in the HOMEMAKER node. When that failed, we attempted to physically reseat it. Since it was the standby card, we did not expect that would cause any problems. However, upon reseating the card, the entire ONS crashed and we lost all traffic through the box. It took more than an hour to recover from this failure.

The worst case scenario is that we have to blow away the entire configuration and start from scratch. Prior to starting our upgrade, we will save the configuration so that if we have to configure the box from scratch, we can simply uploade the saved configuration. We estimate that we will be down for no more than an hour for each node in the system.

Additional Info: 3/26/2013 8:16:13 AM NAME REDACTED

We have tested the upgrade in our lab and it works well. However, we can't repeat the bug in our lab, so we don't know if we will encounter problems when we attempt to upgrade a node that is affected by the bug.

Last CCB Entry: 04/10/13 16:08:11 NAME REDACTED

09 Apr Blarney CCB - Blarney ECP board approved

ECP lead NAME REDACTED

Programs Affected: Blarney Fairview Oakstar Stormbrew

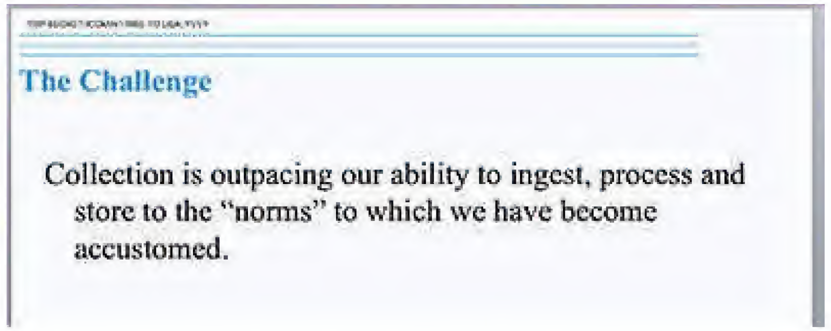
No Related Work Tasks

It is quite possible that Chinese firms are implanting surveillance mechanisms in their network devices. But the United States is certainly doing the same.

Warning the world about Chinese surveillance could have been one of the motives behind the US government's claims that Chinese devices cannot be trusted. But an equally important motive seems to have been preventing Chinese devices from supplanting American-made ones, which would have limited the NSA's own reach. In other words, Chinese routers and servers represent not only economic competition but also surveillance competition: when someone buys a Chinese device instead of an American one, the NSA loses a crucial means of spying on a great many communication activities.

* * *

If the quantity of collection revealed was already stupefying, the NSA's mission to collect all the signals all the time has driven the agency to expand and conquer more and more ground. The amount of data it captures is so vast, in fact, that the principal challenge the agency complains about is storing the heaps of information accumulated from around the globe. One NSA document, prepared for the Five Eyes SigDev Conference, set forth this central problem:

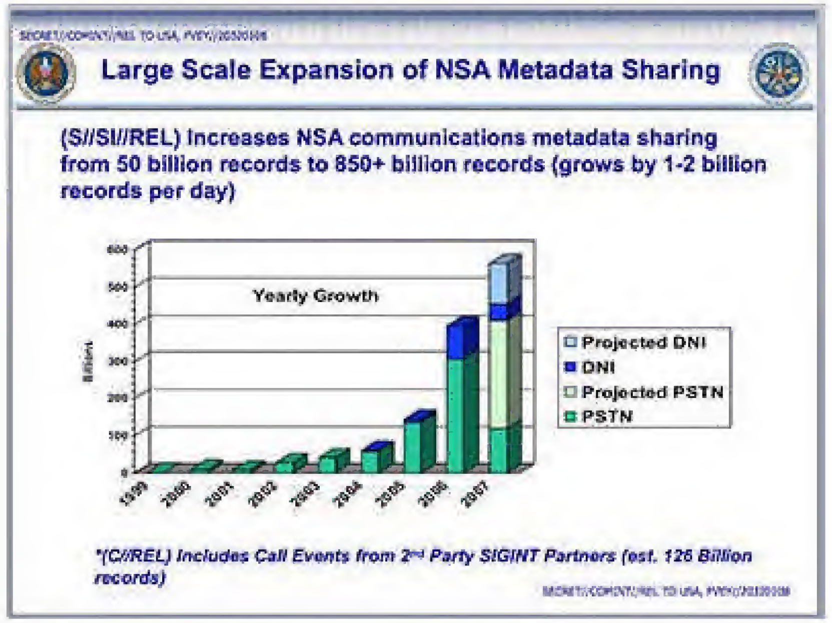


TOP SECRET//COMINT//REL TO USA, FVEY

The Challenge

Collection is outpacing our ability to ingest, process and store to the "norms" to which we have become accustomed.

The story goes back to 2006, when the agency embarked on what it called "Large Scale Expansion of NSA Metadata Sharing." At that point, the NSA predicted that its metadata collection would grow by six hundred billion records every year, growth that would include one to two billion new telephone call events collected every single day:



SECRET//COMINT//REL TO USA, FVEY//20320108

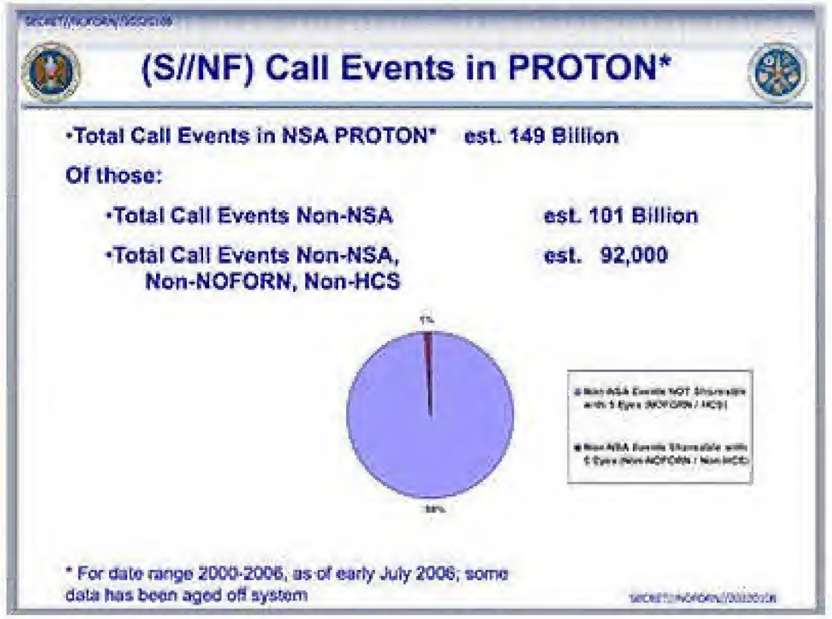
Large Scale Expansion of NSA Metadata Sharing

(S//SI//REL) Increases NSA communications metadata sharing from 50 billion records to 850+ billion records (grows by 1-2 billion records per day)

*(C//REL) Includes Call Events from 2nd Party SIGINT Partners (est. 126 Billion records)

SECRET//COMINT//REL TO USA, FVEY//20320108

By May 2007, the expansion had evidently borne fruit: the amount of telephone metadata the agency was storing—independent of email and other Internet data, and excluding data the NSA had deleted due to lack of storage space—had increased to 150 billion records:



SECRET//NOFORN//20320108

(S//NF) Call Events in PROTON*

•Total Call Events in NSA PROTON* est. 149 Billion

Of those:

•Total Call Events Non-NSA est. 101 Billion

•Total Call Events Non-NSA, Non-NOFORN, Non-HCS est. 92,000

* For date range 2000-2006, as of early July 2006; some data has been aged off system

SECRET//NOFORN//20320108

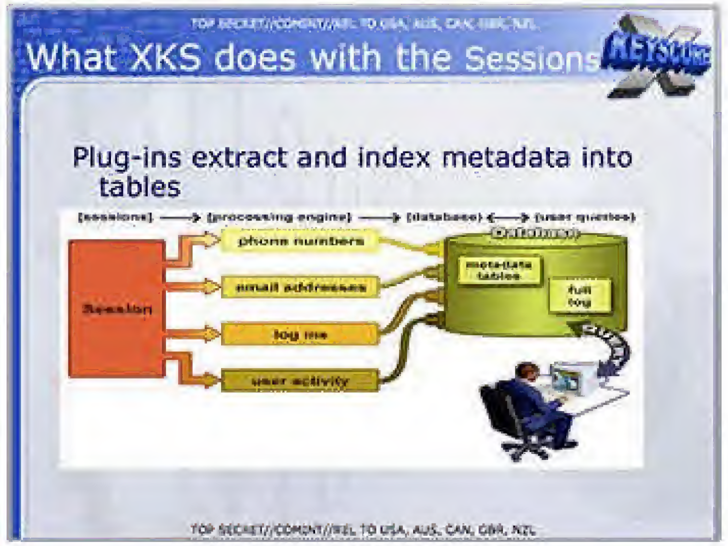
Once Internet-based communications were added to the mix, the total number of communication events stored was close to 1 trillion (this data, it should be noted, was then shared by the NSA with other agencies).

To address its storage problem, the NSA began building a massive new facility in Bluffdale, Utah, that has as one of its primary purposes the retention of all that data. As reporter James Bamford noted in 2012, the Bluffdale construction will expand the agency's capacity by adding "four 25,000-square-foot halls filled with servers, complete with raised floor space for cables and storage. In addition, there will be more than 900,000 square feet for technical support and administration." Considering the size of the building and the fact that, as Bamford says, "a terabyte of data can now be stored on a flash drive the size of a man's pinky," the implications for data collection are profound.

The need for ever-larger facilities is particularly pressing given the agency's current invasions into global online activity, which extend far beyond the collection of metadata to include the actual content of emails, Web browsing, search histories, and chats. The key program used by the NSA to collect, curate, and search such data, introduced in 2007, is X-KEYSCORE, and it affords a radical leap in the scope of the agency's surveillance powers. The NSA calls X-KEYSCORE its "widest-reaching" system for collecting electronic data, and with good reason.

A training document prepared for analysts claims the program captures "nearly everything a typical user does on the internet," including the text of emails, Google searches, and the names of websites visited. X-KEYSCORE even allows "real-time" monitoring of a person's online activities, enabling the NSA to observe emails and browsing activities as they happen.

Beyond collecting comprehensive data about the online activities of hundreds of millions of people, X-KEYSCORE allows any NSA analyst to search the system's databases by email address, telephone number, or identifying attributes such as an IP address. The range of information available and the basic means an analyst uses to search it are illustrated in this slide:



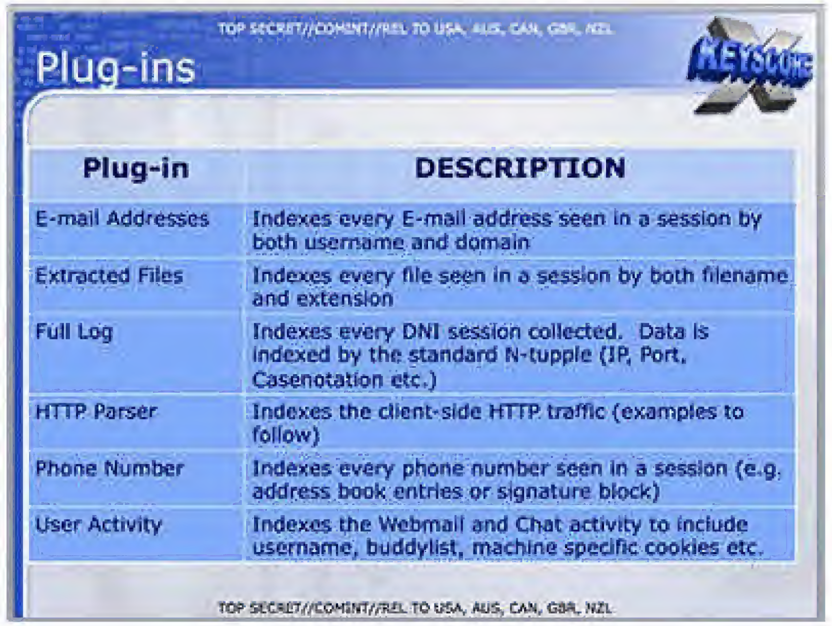
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

What XKS does with the Sessions

Plug-ins extract and index metadata into tables

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Another X-KEYSCORE slide lists the various fields of information that can be searched via the program's "plug-ins." Those include "every email address seen in a session," "every phone number seen in a session" (including "address book entries"), and "the webmail and chat activity":



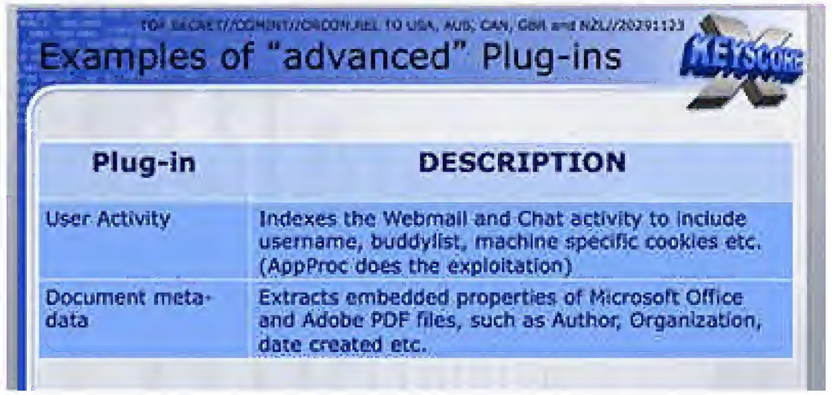
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Plug-ins

Plug-in	DESCRIPTION
E-mail Addresses	Indexes every E-mail address seen in a session by both username and domain
Extracted Files	Indexes every file seen in a session by both filename and extension
Full Log	Indexes every DNI session collected. Data is indexed by the standard N-tupple (IP, Port, Casenotation etc.)
HTTP Parser	Indexes the client-side HTTP traffic (examples to follow)
Phone Number	Indexes every phone number seen in a session (e.g. address book entries or signature block)
User Activity	Indexes the Webmail and Chat activity to include username, buddylist, machine specific cookies etc.

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

The program also offers the ability to search and retrieve embedded documents and images that were created, sent, or received:

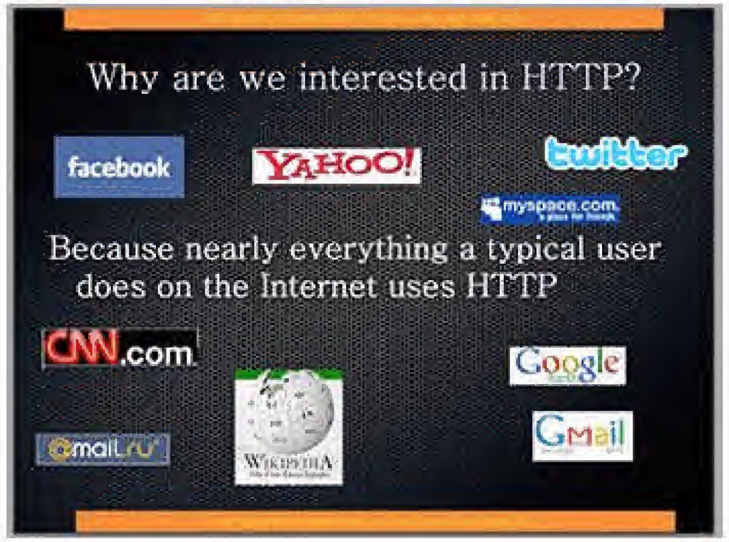


TOP SECRET//COMINT//ORCON,REL TO USA, AUS, CAN, GBR and NZL//20291123

Examples of "advanced" Plug-ins

Plug-in	DESCRIPTION
User Activity	Indexes the Webmail and Chat activity to include username, buddylist, machine specific cookies etc. (AppProc does the exploitation)
Document meta-data	Extracts embedded properties of Microsoft Office and Adobe PDF files, such as Author, Organization, date created etc.

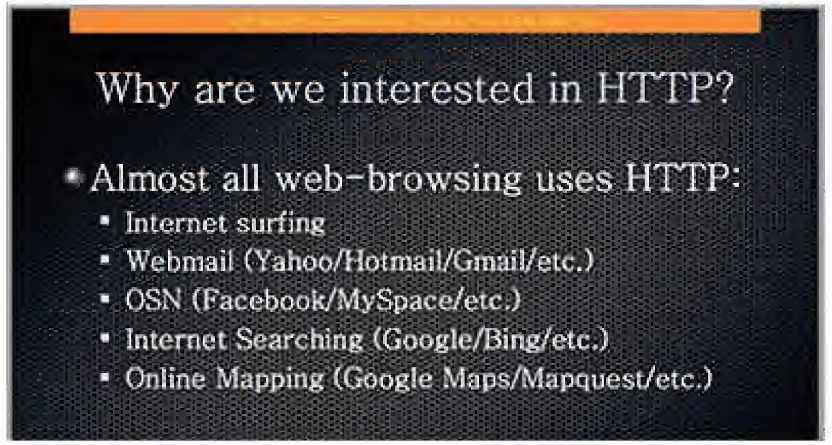
Other NSA slides openly declare the all-encompassing global ambition of X-KEYSCORE:



Why are we interested in HTTP?

Because nearly everything a typical user does on the Internet uses HTTP

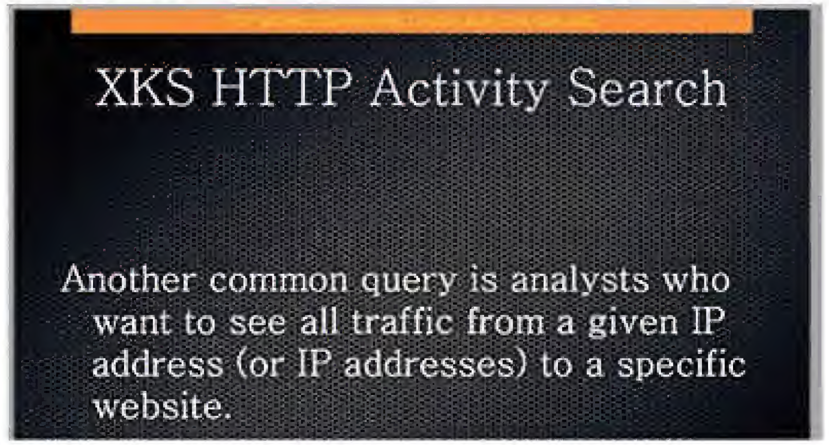
facebook
YAHOO!
twitter
myspace.com
CNN.com
Google
Gmail
@mail.ru
Wikipedia



Why are we interested in HTTP?

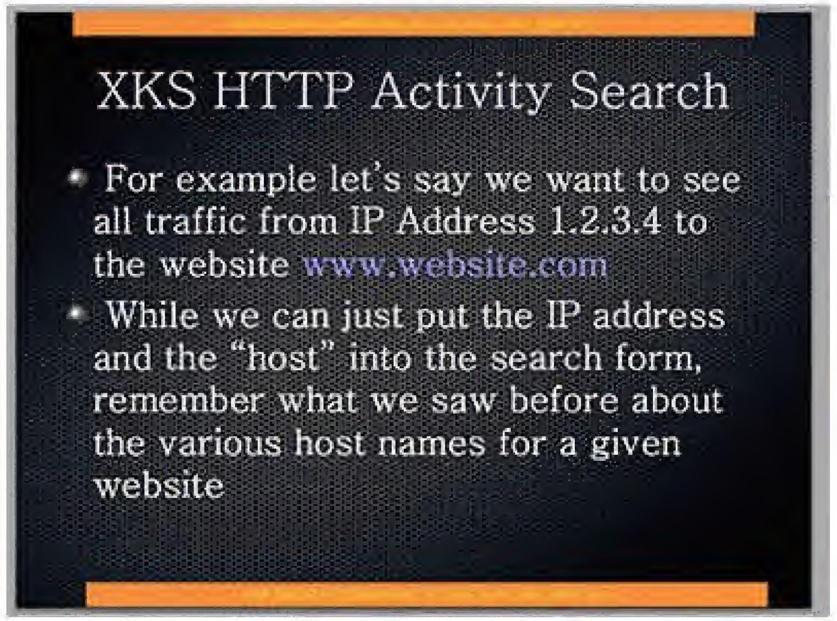
- Almost all web-browsing uses HTTP:
  - Internet surfing
  - Webmail (Yahoo/Hotmail/Gmail/etc.)
  - OSN (Facebook/MySpace/etc.)
  - Internet Searching (Google/Bing/etc.)
  - Online Mapping (Google Maps/Mapquest/etc.)

The searches enabled by the program are so specific that any NSA analyst is able not only to find out which websites a person has visited but also to assemble a comprehensive list of all visits to a particular website from specified computers:



XKS HTTP Activity Search

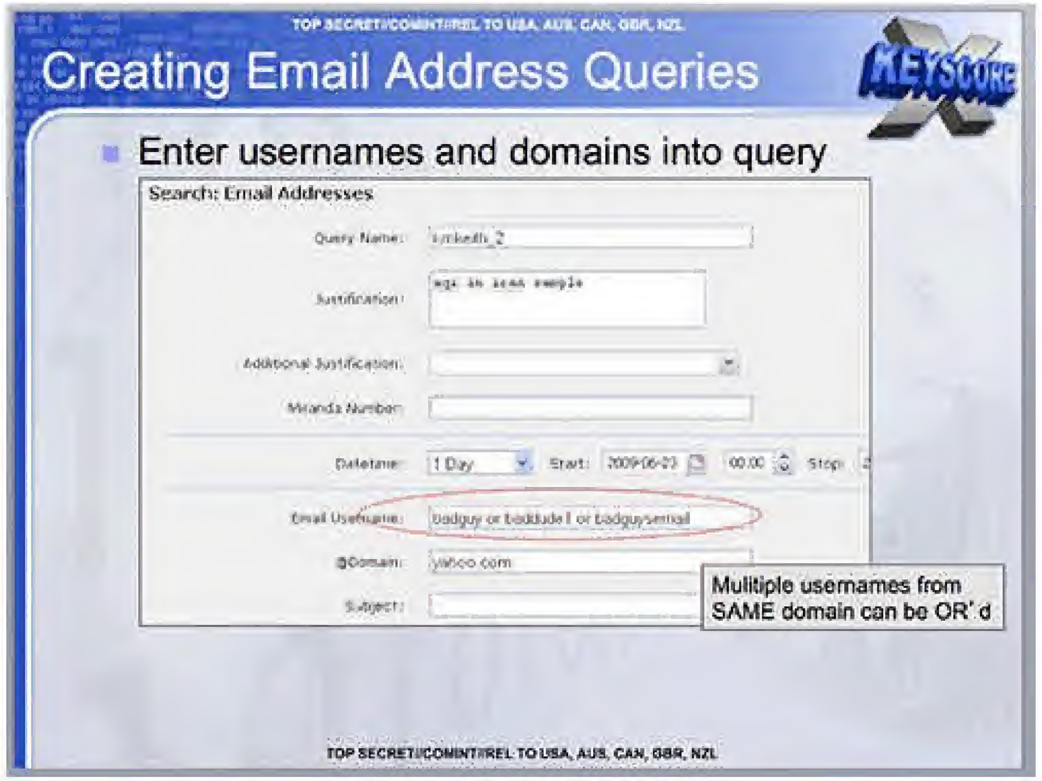
Another common query is analysts who want to see all traffic from a given IP address (or IP addresses) to a specific website.



XKS HTTP Activity Search

- For example let's say we want to see all traffic from IP Address 1.2.3.4 to the website www.website.com
- While we can just put the IP address and the "host" into the search form, remember what we saw before about the various host names for a given website

Most remarkable is the ease with which analysts can search for whatever they want with no oversight. An analyst with access to X-KEYSCORE need not submit a request to a supervisor or any other authority. Instead, the analyst simply fills out a basic form to "justify" the surveillance, and the system returns the information requested.



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Creating Email Address Queries

- Enter usernames and domains into query

Search: Email Addresses

Query Name: umkeith_2

Justification: xks in icon sample

Additional Justification:

Miranda Number:

Datetime: 1 Day Start: 2009-06-23 00:00 Stop:

Email Username: badguy or baddude1 or badguysemail

@Domain: yahoo.com

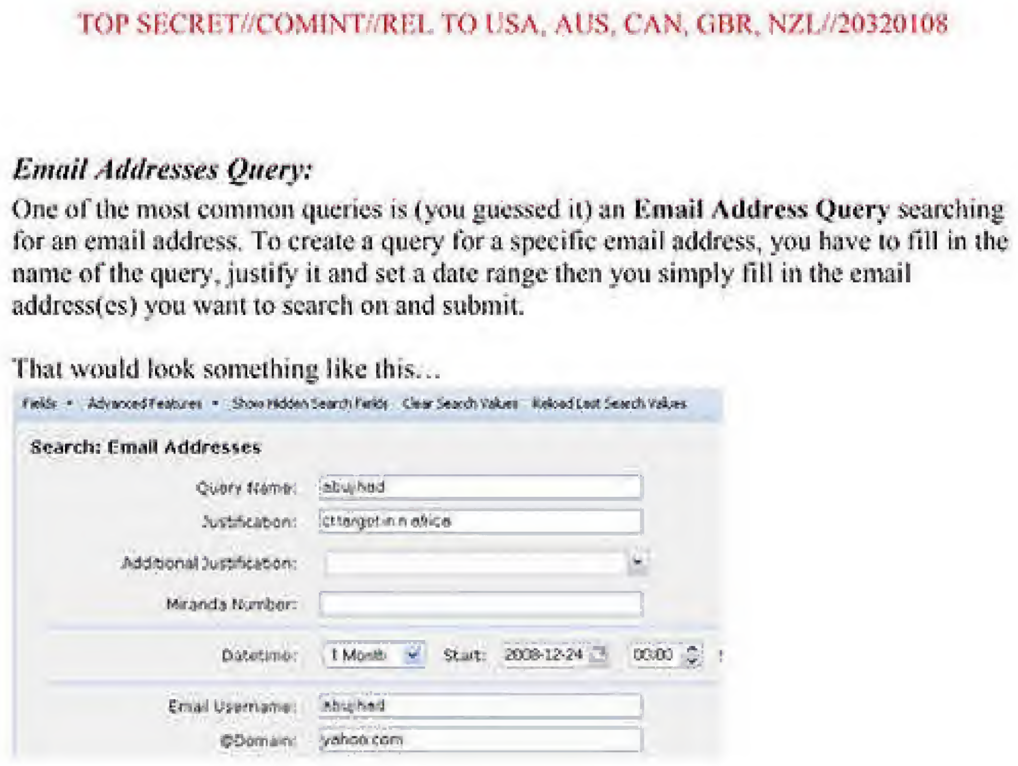
Subject:

Mulitiple usernames from SAME domain can be OR'd

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

In the first video interview he gave when in Hong Kong, Edward Snowden made an audacious claim: "I, sitting at my desk, could wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email." US officials vehemently denied that this was true. Mike Rogers expressly accused Snowden of "lying," adding, "It's impossible for him to do what he was saying he could do." But X-KEYSCORE permits an analyst to do exactly what Snowden said: target any user for comprehensive monitoring, which includes reading the content of their emails. Indeed, the program lets an analyst search for all emails that include targeted users in the "cc" line or mention of them in the body of the text.

The NSA's own instructions for searching through emails demonstrate just how simple and easy it is for analysts to monitor anyone whose address they know:



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108

Email Addresses Query:

One of the most common queries is (you guessed it) an **Email Address Query** searching for an email address. To create a query for a specific email address, you have to fill in the name of the query, justify it and set a date range then you simply fill in the email address(es) you want to search on and submit.

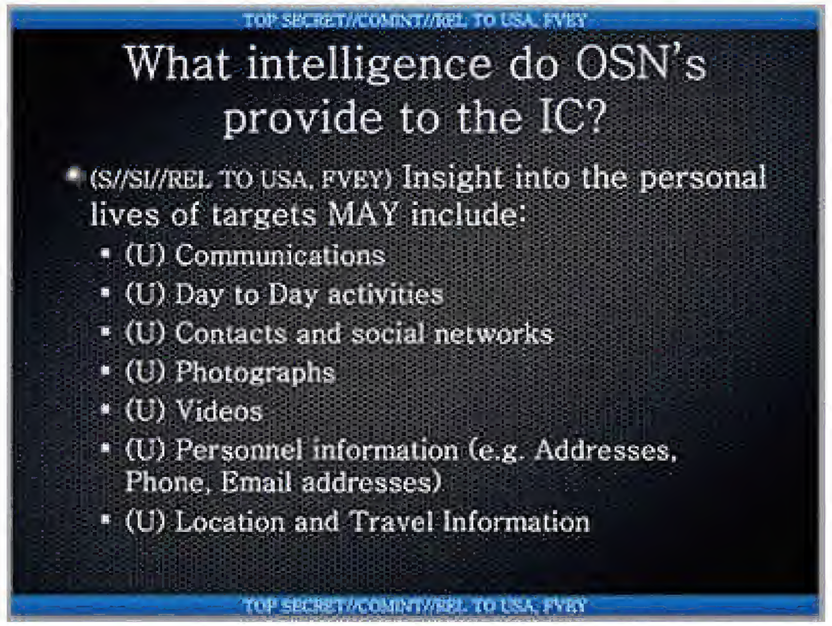
That would look something like this…

Fields • Advanced Features • Show Hidden Search Fields Clear Search Values Reload Last Search Values

Search: Email Addresses

Query Name: abujhad
Justification: cttarget in n africa
Additional Justification:
Miranda Number:
Datetime: 1 Month Start: 2008-12-24 00:00
Email Username: abujhad
@Domain: yahoo.com

One of X-KEYSCORE's most valuable functions to the NSA is its ability to surveil the activities on online social networks (OSNs), such as Facebook and Twitter, which the agency believes provide a wealth of information and "insight into the personal lives of targets:"



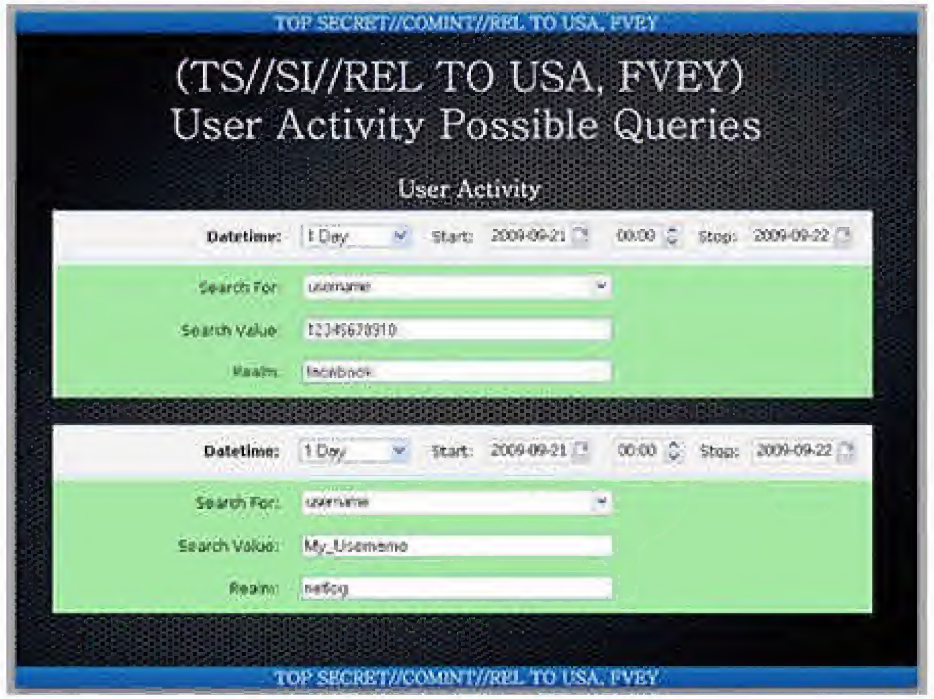
TOP SECRET//COMINT//REL TO USA, FVEY

What intelligence do OSN's provide to the IC?

- (S//SI//REL TO USA, FVEY) Insight into the personal lives of targets MAY include:
  - (U) Communications
  - (U) Day to Day activities
  - (U) Contacts and social networks
  - (U) Photographs
  - (U) Videos
  - (U) Personnel information (e.g. Addresses, Phone, Email addresses)
  - (U) Location and Travel Information

TOP SECRET//COMINT//REL TO USA, FVEY

The methods for searching social media activity are every bit as simple as the email search. An analyst enters the desired user name on, say, Facebook, along with the date range of activity, and X-KEYSCORE then returns all of that user's information, including messages, chats, and other private postings.



TOP SECRET//COMINT//REL TO USA, FVEY

(TS//SI//REL TO USA, FVEY)
User Activity Possible Queries

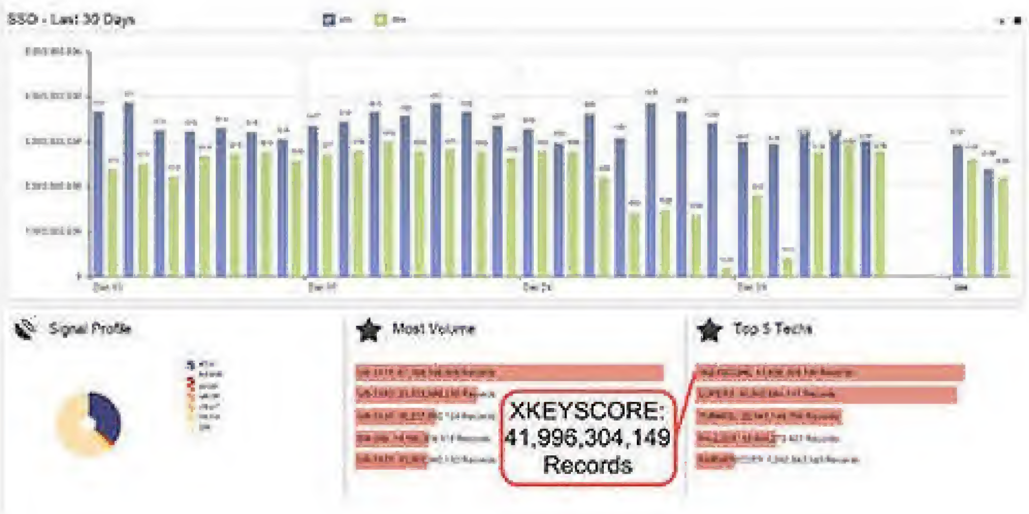
User Activity

Datetime: 1 Day Start: 2009-09-21 00:00 Stop: 2009-09-22
Search For: username
Search Value: 12345678910
Realm: facebook

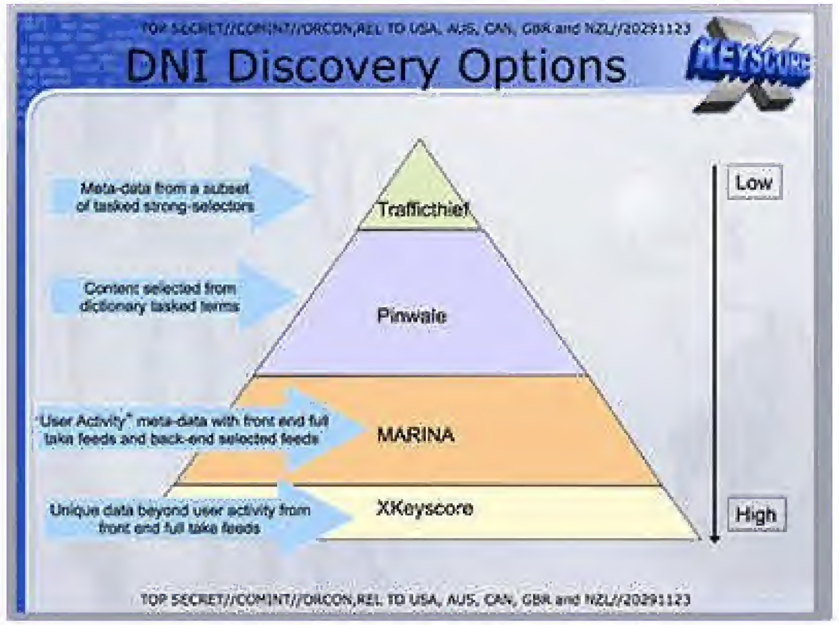
Datetime: 1 Day Start: 2009-09-21 00:00 Stop: 2009-09-22
Search For: username
Search Value: My_Username
Realm: netlog

TOP SECRET//COMINT//REL TO USA, FVEY

Perhaps the most remarkable fact about X-KEYSCORE is the sheer quantity of data that it captures and stores at multiple collection sites around the world. "At some sites," one report states, "the amount of data we receive per day (20+ terabytes) can only be stored for as little as 24 hours based on available resources." For one thirty-day period beginning in December 2012, the quantity of records collected by X-KEYSCORE just for one unit, the SSO, exceeded forty-one billion:



X-KEYSCORE "stores the full-take content for 3–5 days, effectively 'slowing down the internet,'"—meaning that "analysts can go back and recover sessions." Then "content that is 'interesting' can be pulled out of X-KEYSCORE and pushed to Agility or PINWALE," storage databases that provide longer retention.



TOP SECRET//COMINT//ORCON,REL TO USA, AUS, CAN, GBR and NZL//20291123

DNI Discovery Options

Meta-data from a subset of tasked strong-selectors

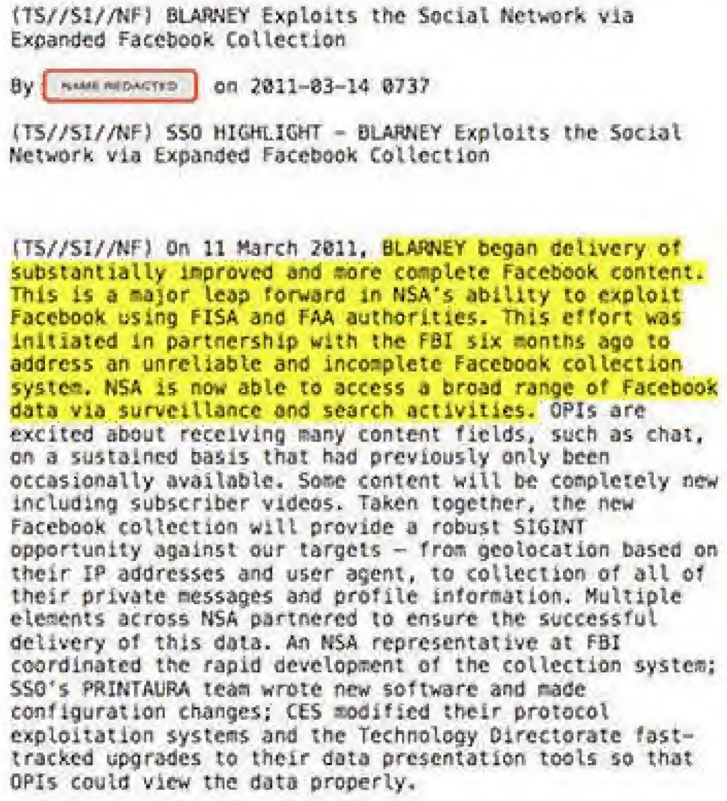
Content selected from dictionary tasked terms

"User Activity" meta-data with front end full take feeds and back-end selected feeds

Unique data beyond user activity from front end full take feeds

TOP SECRET//COMINT//ORCON,REL TO USA, AUS, CAN, GBR and NZL//20291123

X-KEYSCORE's ability to access Facebook and other social media sites is boosted by other programs, which include BLARNEY, allowing the NSA to monitor a "broad range of Facebook data via surveillance and search activities":



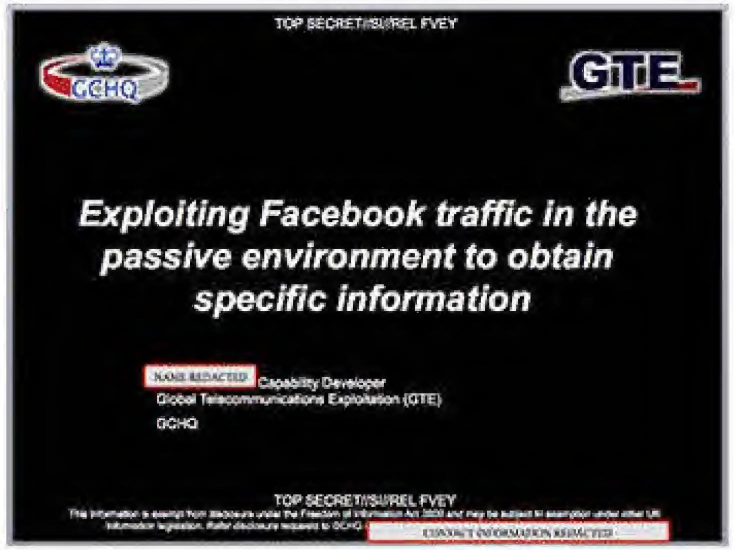
(TS//SI//NF) BLARNEY Exploits the Social Network via Expanded Facebook Collection

By NAME REDACTED on 2011-03-14 0737

(TS//SI//NF) SSO HIGHLIGHT - BLARNEY Exploits the Social Network via Expanded Facebook Collection

(TS//SI//NF) On 11 March 2011, BLARNEY began delivery of substantially improved and more complete Facebook content. This is a major leap forward in NSA's ability to exploit Facebook using FISA and FAA authorities. This effort was initiated in partnership with the FBI six months ago to address an unreliable and incomplete Facebook collection system. NSA is now able to access a broad range of Facebook data via surveillance and search activities. OPIs are excited about receiving many content fields, such as chat, on a sustained basis that had previously only been occasionally available. Some content will be completely new including subscriber videos. Taken together, the new Facebook collection will provide a robust SIGINT opportunity against our targets – from geolocation based on their IP addresses and user agent, to collection of all of their private messages and profile information. Multiple elements across NSA partnered to ensure the successful delivery of this data. An NSA representative at FBI coordinated the rapid development of the collection system; SSO's PRINTAURA team wrote new software and made configuration changes; CES modified their protocol exploitation systems and the Technology Directorate fast-tracked upgrades to their data presentation tools so that OPIs could view the data properly.

In the UK, meanwhile, the GCHQ's Global Telecommunications Exploitation (GTE) division has also devoted substantial resources to the task, detailed in a 2011 presentation to the annual Five Eyes conference.

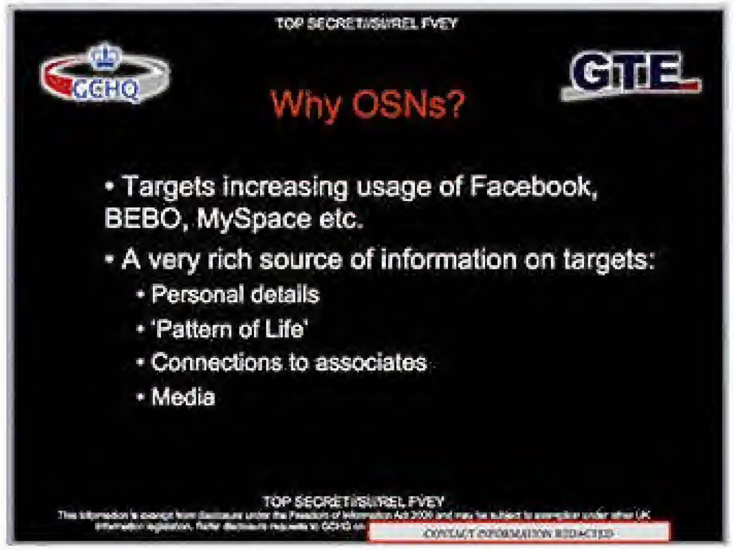


TOP SECRET//SI//REL FVEY

Exploiting Facebook traffic in the passive environment to obtain specific information

NAME REDACTED Capability Developer
Global Telecommunications Exploitation (GTE)
GCHQ

TOP SECRET//SI//REL FVEY
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED



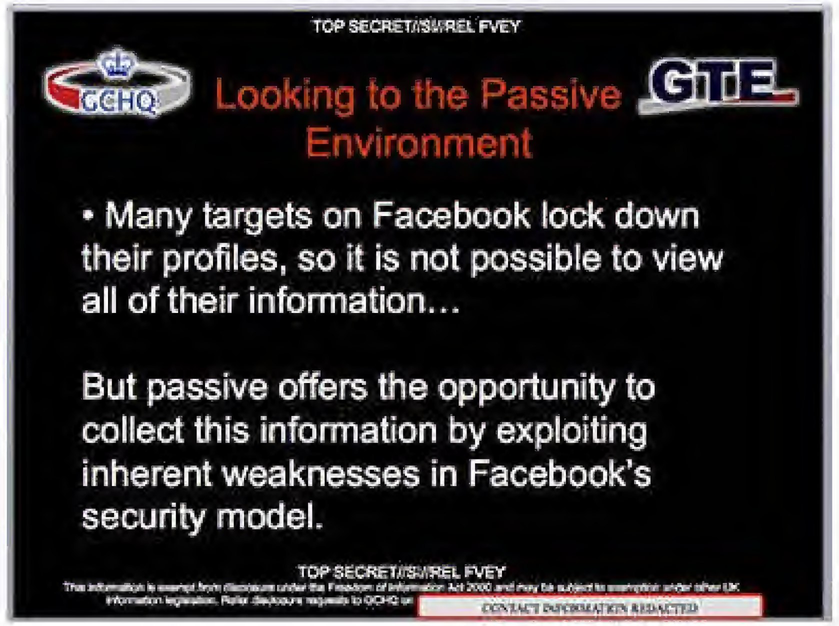
TOP SECRET//SI//REL FVEY

Why OSNs?

- Targets increasing usage of Facebook, BEBO, MySpace etc.
- A very rich source of information on targets:
  - Personal details
  - 'Pattern of Life'
  - Connections to associates
  - Media

TOP SECRET//SI//REL FVEY
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED

The GCHQ has paid special attention to weaknesses in Facebook's security system and to obtaining the kind of data that Facebook users attempt to shield:



TOP SECRET//SI//REL FVEY

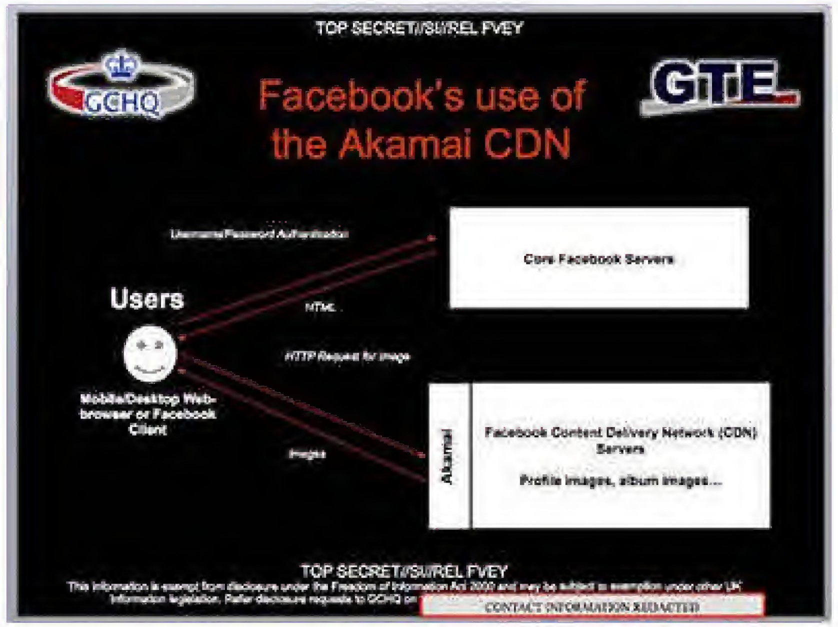
Looking to the Passive Environment

- Many targets on Facebook lock down their profiles, so it is not possible to view all of their information…

But passive offers the opportunity to collect this information by exploiting inherent weaknesses in Facebook's security model.

TOP SECRET//SI//REL FVEY
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED

In particular, the GCHQ has found vulnerabilities in the network's system for storing pictures, which can be used to gain access to Facebook IDs and album images:

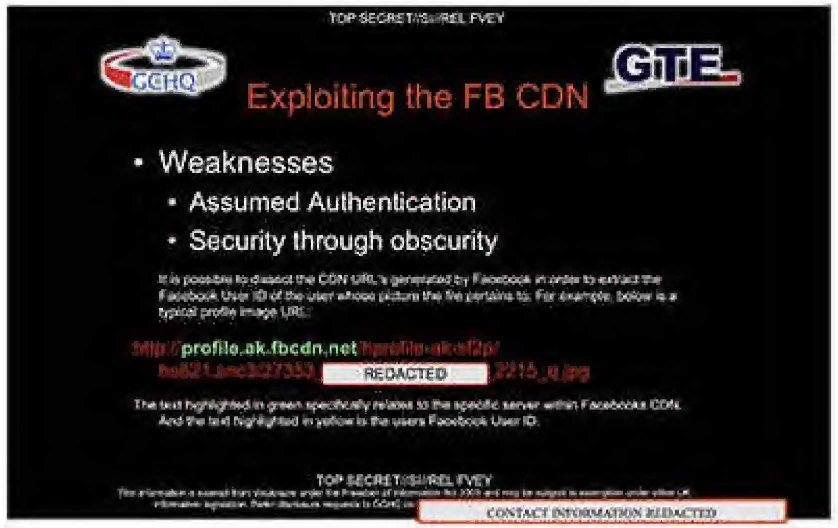


TOP SECRET//SI//REL FVEY

Facebook's use of the Akamai CDN

Username/Password Authentication
Core Facebook Servers
Users
HTML
HTTP Request for image
Mobile/Desktop Web-browser or Facebook Client
Images
Akamai
Facebook Content Delivery Network (CDN) Servers
Profile images, album images…

TOP SECRET//SI//REL FVEY
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED



TOP SECRET//SI//REL FVEY

Exploiting the FB CDN

- Weaknesses
  - Assumed Authentication
  - Security through obscurity

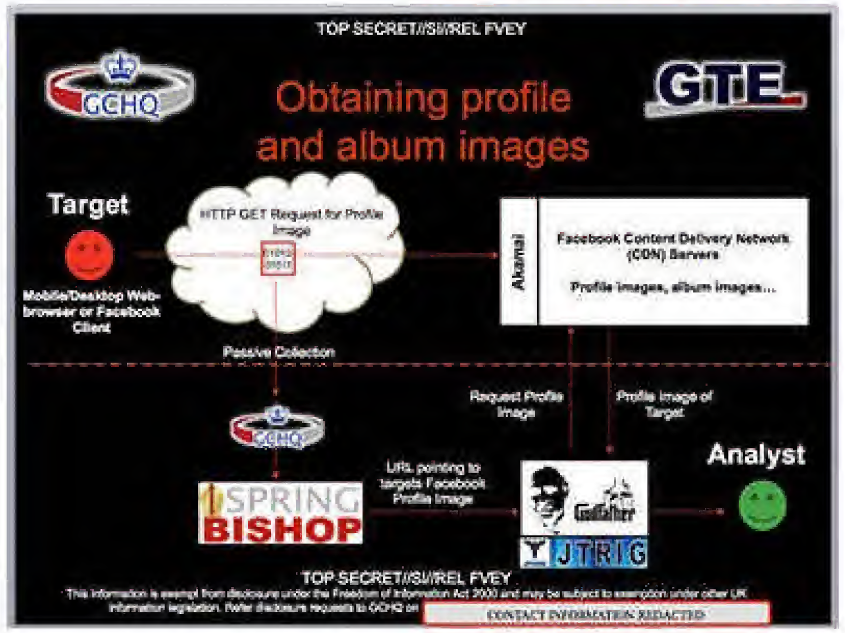
It is possible to dissect the CDN URL's generated by Facebook in order to extract the Facebook User ID of the user whose picture the file pertains to. For example, below is a typical profile image URL:

http://profile.ak.fbcdn.net/hprofile-ak-ash2/ hs621.snc3/27353 REDACTED 2215_q.jpg

The text highlighted in green specifically relates to the specific server within Facebooks CDN. And the text highlighted in yellow is the users Facebook User ID.

TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED



TOP SECRET//SI//REL FVEY

Obtaining profile and album images

Target
Mobile/Desktop Web-browser or Facebook Client
HTTP GET Request for Profile Image
Akamai
Facebook Content Delivery Network (CDN) Servers
Profile images, album images...
Passive Collection
Request Profile Image
Profile image of Target
Analyst
SPRING BISHOP
URL pointing to targets Facebook Profile Image
Godfather
JTRIG

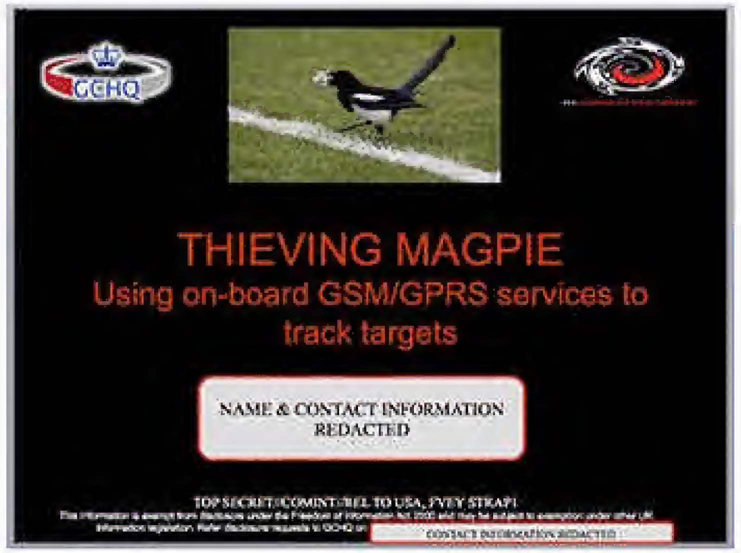
TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED

Beyond social media networks, the NSA and the GCHQ continue to look for any gaps in their surveillance net, any communications that remain outside their grasp, and then develop ways to bring them under the agencies' watchful eye. One seemingly obscure program demonstrates this point.

Both the NSA and GCHQ have been consumed by their perceived need to monitor Internet and phone communications of people on commercial airline flights. Because these are rerouted via independent satellite systems, they are extremely difficult to pinpoint. The idea that there is a moment when someone can use the Internet or their phone without detection—even for just a few hours while flying—is intolerable to the surveillance agencies. In response, they have devoted substantial resources to developing systems that will intercept in-flight communications.

At the 2012 Five Eyes conference, the GCHQ presented an interception program named Thieving Magpie, targeting the increasingly available use of cell phones during flights:



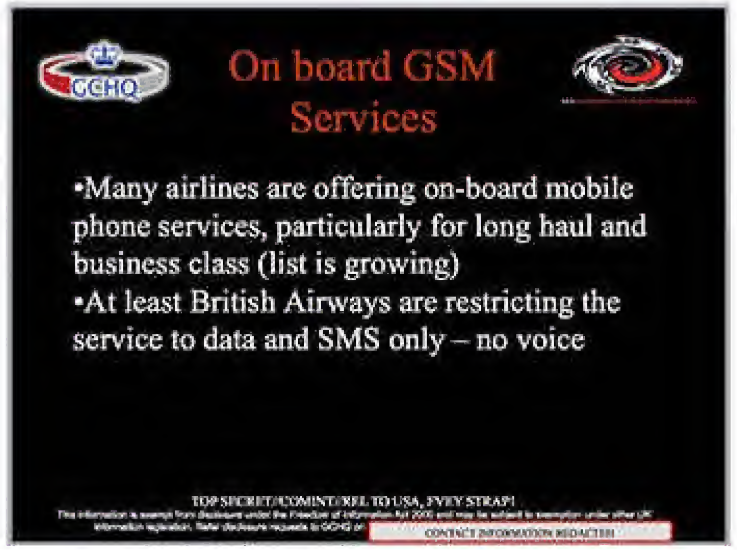
THIEVING MAGPIE

Using on-board GSM/GPRS services to track targets

NAME & CONTACT INFORMATION REDACTED

TOP SECRET//COMINT//REL TO USA, FVEY STRAP1

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED



On board GSM Services

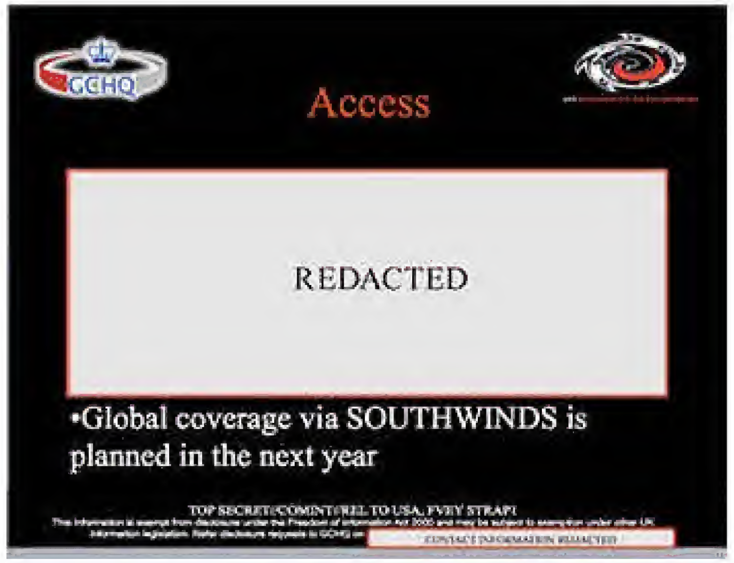
•Many airlines are offering on-board mobile phone services, particularly for long haul and business class (list is growing)

•At least British Airways are restricting the service to data and SMS only – no voice

TOP SECRET//COMINT//REL TO USA, FVEY STRAP1

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED

The proposed solution envisioned a system to ensure complete "global coverage":



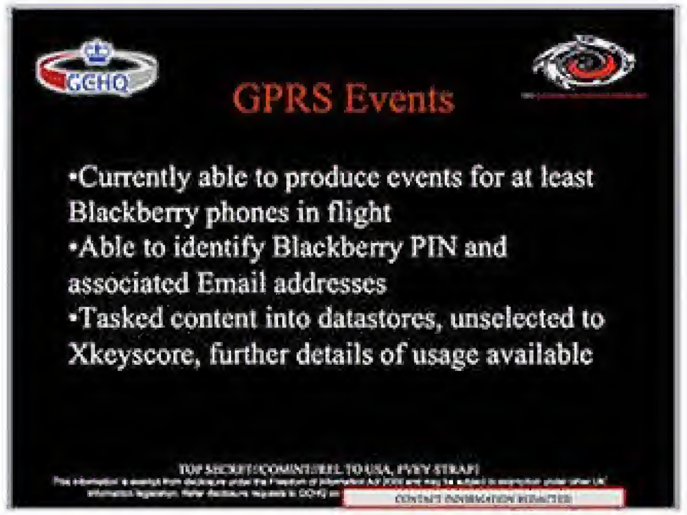
Access

REDACTED

- Global coverage via SOUTHWINDS is planned in the next year

TOP SECRET//COMINT//REL TO USA, FVEY STRAP1
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED

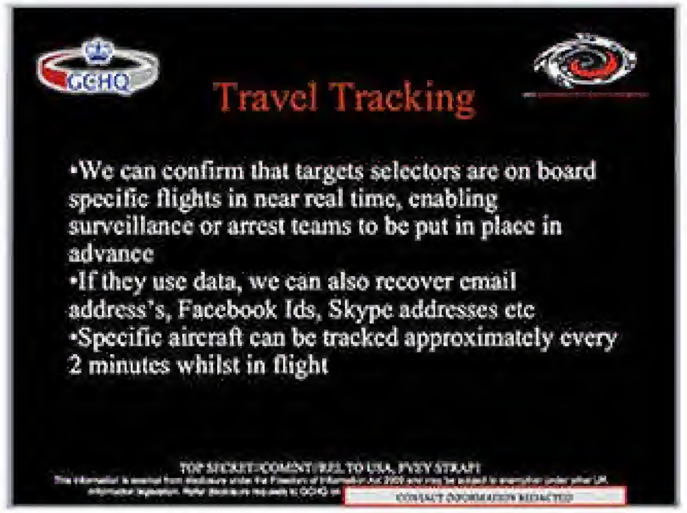
Substantial headway has been made to ensure that certain devices are susceptible to surveillance on passenger jets:



GPRS Events

- Currently able to produce events for at least Blackberry phones in flight
- Able to identify Blackberry PIN and associated Email addresses
- Tasked content into datastores, unselected to Xkeyscore, further details of usage available

TOP SECRET//COMINT//REL TO USA, FVEY STRAP1
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED

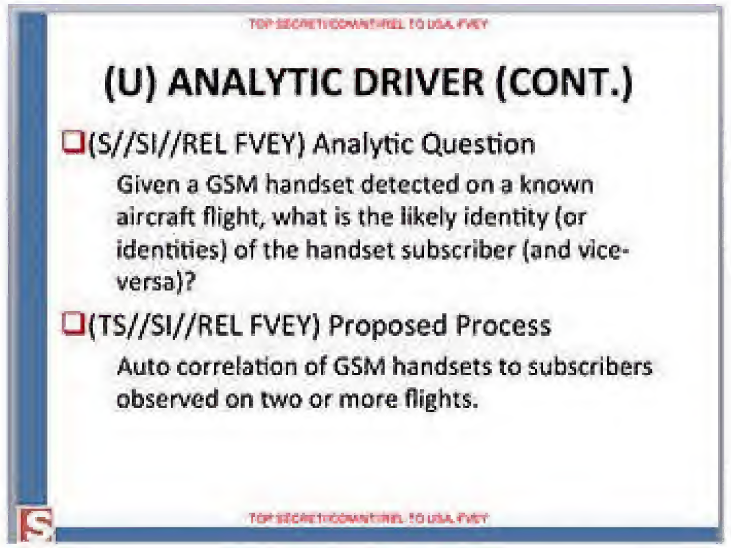


Travel Tracking

- We can confirm that targets selectors are on board specific flights in near real time, enabling surveillance or arrest teams to be put in place in advance
- If they use data, we can also recover email address's, Facebook Ids, Skype addresses etc
- Specific aircraft can be tracked approximately every 2 minutes whilst in flight

TOP SECRET//COMINT//REL TO USA, FVEY STRAP1
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED

A related NSA document presented at the same conference, for a program entitled Homing Pigeon, also describes efforts to monitor in-air communications. The agency's program was to be coordinated with the GCHQ, and the entire system made available to the Five Eyes group.



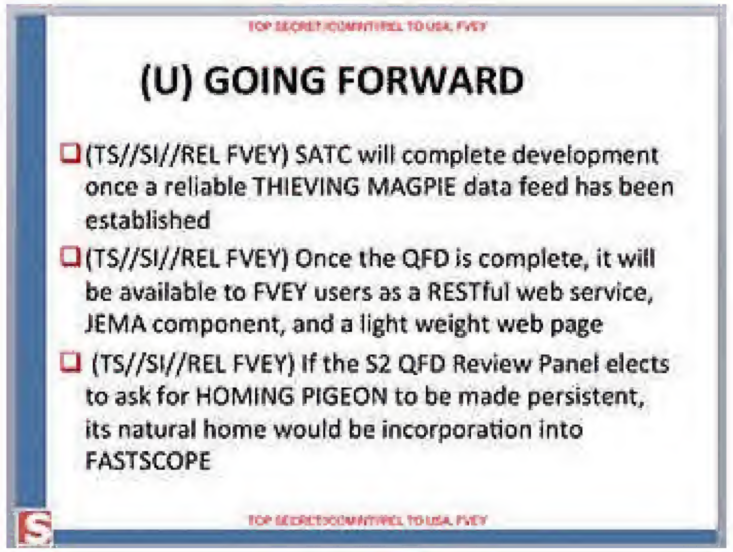
TOP SECRET//COMINT//REL TO USA, FVEY

(U) ANALYTIC DRIVER (CONT.)

❑(S//SI//REL FVEY) Analytic Question
Given a GSM handset detected on a known aircraft flight, what is the likely identity (or identities) of the handset subscriber (and vice-versa)?

❑(TS//SI//REL FVEY) Proposed Process
Auto correlation of GSM handsets to subscribers observed on two or more flights.

TOP SECRET//COMINT//REL TO USA, FVEY



TOP SECRET//COMINT//REL TO USA, FVEY

(U) GOING FORWARD

❑(TS//SI//REL FVEY) SATC will complete development once a reliable THIEVING MAGPIE data feed has been established

❑(TS//SI//REL FVEY) Once the QFD is complete, it will be available to FVEY users as a RESTful web service, JEMA component, and a light weight web page

❑ (TS//SI//REL FVEY) If the S2 QFD Review Panel elects to ask for HOMING PIGEON to be made persistent, its natural home would be incorporation into FASTSCOPE

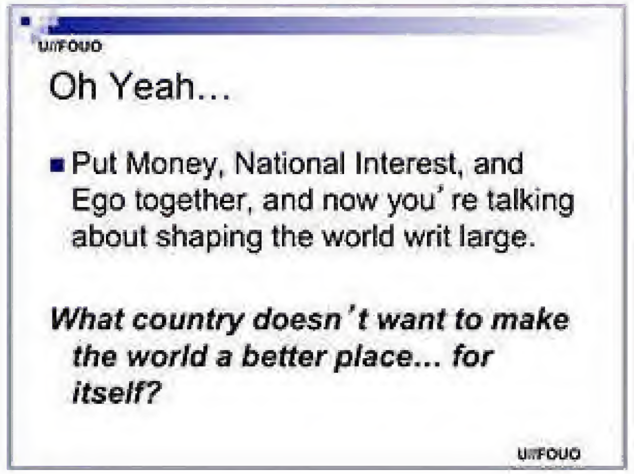
TOP SECRET//COMINT//REL TO USA, FVEY

* * *

There is remarkable candidness, within parts of the NSA, about the true purpose of building so massive a secret surveillance system. A PowerPoint presentation prepared for a group of agency officials discussing the prospect of international Internet standards gives the unvarnished view.

The author of the presentation is an "NSA/SIGINT National Intelligence Officer (SINIO) for Science and Technology," a self-described "well trained scientist and hacker."

The blunt title of his presentation: "The Role of National Interests, Money, and Egos." These three factors together, he says, are the primary motives driving the United States to maintain global surveillance domination.



U//FOUO

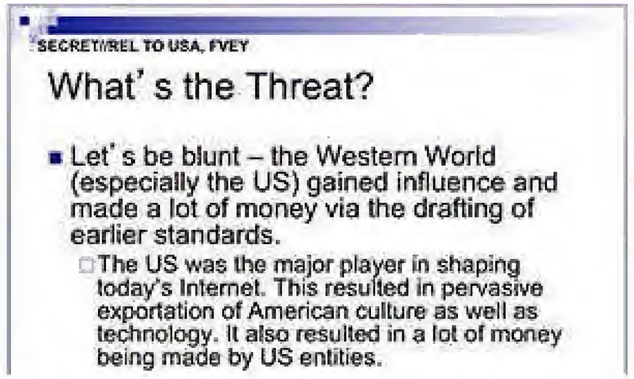
Oh Yeah...

- Put Money, National Interest, and Ego together, and now you're talking about shaping the world writ large.

What country doesn't want to make the world a better place... for itself?

U//FOUO

He notes that US dominance over the Internet has given the country substantial power and influence, and has also generated vast profit:



SECRET//REL TO USA, FVEY

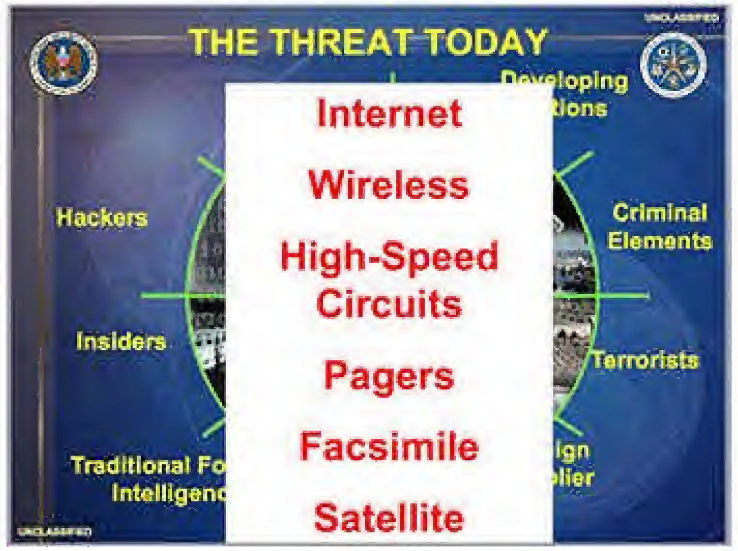
What's the Threat?

- Let's be blunt – the Western World (especially the US) gained influence and made a lot of money via the drafting of earlier standards.
  - The US was the major player in shaping today's Internet. This resulted in pervasive exportation of American culture as well as technology. It also resulted in a lot of money being made by US entities.

Such profit and power have also inevitably accrued, of course, to the surveillance industry itself, providing another motive for its endless expansion. The post-9/11 era has seen a massive explosion of resources dedicated to surveillance. Most of those resources were transferred from the public coffers (i.e., the American taxpayer) into the pockets of private surveillance defense corporations.

Companies like Booz Allen Hamilton and AT&T employ hordes of former top government officials, while hordes of current top defense officials are past (and likely future) employees of those same corporations. Constantly growing the surveillance state is a way to ensure that the government funds keep flowing, that the revolving door stays greased. That is also the best way to ensure that the NSA and its related agencies retain institutional importance and influence inside Washington.

As the scale and ambition of the surveillance industry has grown, so has the profile of its perceived adversary. Listing the various threats supposedly facing the United States, the NSA—in a document entitled "National Security Agency: Overview Briefing"—includes some predictable items: "hackers," "criminal elements," and "terrorists." Revealingly, though, it also goes far broader by including among the threats a list of *technologies,* including the Internet itself:



UNCLASSIFIED

THE THREAT TODAY

Developing
tions

Hackers

Criminal Elements

Insiders

Terrorists

Traditional Fo
Intelligenc

ign
lier

Internet

Wireless

High-Speed Circuits

Pagers

Facsimile

Satellite

UNCLASSIFIED

The Internet has long been heralded as an unprecedented instrument of democratization and liberalization, even emancipation. But in the eyes of the US government, this global network and other types of communications technology threaten to undermine American power. Viewed from this perspective, the NSA's ambition to "collect it all" at last becomes coherent. It is vital that the NSA monitor all parts of the Internet and any other means of communication, so that none can escape US government control.

Ultimately, beyond diplomatic manipulation and economic gain, a system of ubiquitous spying allows the United States to maintain its grip on the world. When the United States is able to know everything that everyone is doing, saying, thinking, and planning—its own citizens, foreign populations, international corporations, other government leaders—its power over those factions is maximized. That's doubly true if the government operates at ever greater levels of secrecy. The secrecy creates a one-way mirror: the US government sees what everyone else in the world does, including its own population, while no one sees its own actions. It is the ultimate imbalance, permitting the most dangerous of all human conditions: the exercise of limitless power with no transparency or accountability.

Edward Snowden's revelations subverted that dangerous dynamic by shining a light on the system and how it functions. For the first time, people everywhere were able to learn the true extent of the surveillance capabilities amassed against them. The news triggered an intense, sustained worldwide debate precisely because the surveillance poses such a grave threat to democratic governance. It also triggered proposals for reform, a global discussion of the importance of Internet freedom and privacy in the electronic age, and a reckoning with the vital question: What does limitless surveillance mean for us as individuals, in our own lives?